DYNASTAR 100/100i/100e/2000/500/5000™
INSTALLATION AND USER GUIDE

JANUARY 2003

VERSION 6.09

GarrettCom®

Industrial Networking at Its Best℠

www.garrettcom.com

Garrettcom, Inc.
25 Commerce Way #1
North Andover, MA 01845
USA
Phone: (978) 688-8807
Fax: (978) 688-8771

Virginia Facility
10222 Battleview Parkway
Manassas, VA 20109-2336
USA
Phone: (703) 257-8900
Fax: (703) 366-3200

620-0220-001 Rev B

$5.00 USD

DynaStar Multi-Service Switches Installation and User Guide

Document Part Number and Revision:

This document describes the features, functions, configuration parameters and statistics displays for the *DYNASTAR* series of Multi-Service Switches. For ordering, use kit part number *160-1300-001*.

DYMEC-DynaStar Stock Number: *620-0220-001*

Revision History:

Date	**Document Revision**	**Software Releases**
April 2000	A	6.06
June 2000	B	6.06
October 2002	C	6.09

Copyright Notices:

FCC Warning:

This equipment has been tested and found to comply with the limits for Class A digital devices, pursuant to Part 15 Subpart J of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Changes or modifications not expressly approved by DYMEC-DynaStar, Inc. could void the user's authority to operate the equipment.

English Text (UL/CSA)	***German Text (VDE/TUV)***	***French Text***
WARNING Access to the interior of this unit shall be made only by a qualified technician. 1. To ensure adequate cooling of the equipment, a 2.0 inch unobstructed space must be provided around all sides of the unit. 2. The AC Power Socket shall be installed near the equipment and shall be easily accessible.	**WARNUNG** Der Zugang ins Innere des Gerätes ist nur einem fachlich qualifizierten Techniker gestattet. 1. Um die Kühlung des Gerätes nicht zu beeinträchtigen, ist es notwendig, an allen Seiten des Gerätes ca. 5 cm Raum zu lassen. 2. Stellen Sie das Gerät in der Nähe eines geerdeten Schutzkontaktsteckers so auf, dass der Stecker leicht erreichbar und zugänglich ist.	**AVERTISSEMENT** Seul un spécialiste devrait avoir accès à l'appareil. 1. Afin de ne pas nuire au processus de refroidissement, il est nécessaire de laisser un espace d'environ 5 cm de chaque côté de l'appareil. 2. Placez l'appareil près d'une prise de courant facilement accessible.

English Text (UL/CSA)	***German Text (VDE/TUV)***	***French Text***
WARNING Remove power plug from the power socket before performing any service work on the unit!	**WARNUNG** Vorm Öffnen des Gerätes muss der Netzstecker vom Strom-netz getrennt werden!	**AVERTISSEMENT** Débranchez l'appareil avant de l'ouvrir.

CAUTION: Service of this unit can be made only by factory authorized service personnel. Failure to observe this warning can result in malfunction to the unit as well as electrocution to personnel.

AVERTISSEMENT:
Cet appareil ne peut être examiné ou réparé que par un employé autorisé du fabricant. Si cette consigne n'est pas respectée, il y a risque de panne et d'électrocution.

VORSICHT: Dieses Gerät darf nur durch das bevollmächtigte Kundendienstpersonal der fabrik instandgehalten werden. Die Nichtbeachtung dieserVorschrift kann zu Fehlfunktionen des Gerätes führen und das Personal durch Stromschläge gefährden.

Industry Canada Warnings	Avis d’Industrie Canada
Notice: The Industry Canada label identifies certified equipment. This certification means that the equipment meets telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the equipment will operate to the user’s satisfaction. Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations. Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment. Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. The precaution may be particularly important in rural areas.	Avis: L’étiquette d’Industrie Canada identifie le matériel homologué. Cette étiquette certifie que le matériel est conforme aux normes de protection, d’exploitation et de sécurité des réseaux de télécommunications, comme le prescrivent les documents concernant les exigences techniques relatives au matériel terminal. Le Ministère n’assure toutefois pas que le matériel fonctionnera à la satisfaction de l’utilisateur. Avant d’installer ce matériel, l’utilisateur doit s’assurer qu’il est permis de le raccorder aux installations de l’entreprise locale de télécommunication. Le matériel doit également être installé en suivant une méthode acceptée de raccordement. L’abonné ne doit pas oublier qu’il est possible que la conformité aux conditions énoncées ci-dessus n’empêche pas la dégradation du service dans certaines situations. Les réparations de matériel homologué doivent être coordonnées par un représentant désigné par le fournisseur. L’entreprise de télécommunications peut demander à l’utilisateur de débrancher un appareil à la suite de réparations ou de modifications effectuées par l’utilisateur ou à cause de mauvais fonctionnement.

Industry Canada Warnings	Avis d’Industrie Canada
Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority or electrician, as appropriate.	Pour sa propre protection, l’utilisateur doit s’assurer que tous les fils de mise à la terre de la source d’énergie électrique, des lignes téléphoniques et des canalisations d’eau métalliques, s’il y en a, sont raccordés ensemble. Cette précaution est particulièrement importante dans les régions rurales.

NOTICE: All specifications, tolerances, and product characteristics are subject to change without notice.

Service Personnel Warning

The *DYNASTAR* may be equipped with dual AC or DC power cords. Remove all AC power cables from the unit and disable all DC power connections at the circuit panel before servicing the unit.

Caution: The installation of this product must comply with all applicable codes and practices specified by the country, city, and operating company in which it is installed.

UL Requirements (US and Canada)

For units set at 120V, use a listed cord set consisting of a minimum No. 18 AWG (.83 mm^2), Type SVT or SJT three-conductor cord a maximum of 15 ft. in length and a parallel blade, grounding type attachment, rated at 15A, 125V.

For units set at 240V, world-wide requirements, use a UL listed cord set consisting of a minimum No. 18 AWG (.83 mm^2) cord and grounding type attachment, rated at 15A, 240V that has the appropriate safety approvals for the country in which the equipment is to be installed and is marked HAR.

Conformité UL (E.-U. et Canada)

Dans le cas des unités devant fonctionner sous 120 V c.a., utilisez un cordon d’alimentation homologue UL constitué au minimum d’un cordon de calibre 18 AWG (0,83 mm^3) de type SVT ou SJT à trois conducteurs d’une longueur maximale de 15 pieds muni d’une prise à lames parallèles avec mise à la terre et pouvant supporter 15 A à 125 V. Dans le cas des unités devant fonctionner sous 250 V c.a. conformément aux normes internationales, utilisez un cordon d’alimentation homologue UL constitué au minimum d’un cordon de calibre 18 AWG (0,83 mm^3) muni d’une prise avec mise à la terre pouvant supporter 15 A à 240 V, marqué HAR et conforme aux normes de securité en vigueur dans le pays où le materiel doit être utilisé.

European Standard EN41003

As per European Standard EN41003, Clause 4.1.3, all the ports of the *DYNASTAR* are SELV circuits and must be connected only to similar SELV circuits, except for certain TNV ports described herein, which must be connected to like circuits.

Europäische Norm

Nach der europäischen Norm EN41003 Absatz 4.1.3 sind alle Anschlüsse von *DYNASTAR* SELV-Stromkreise und müssen nur an gleichwertigen SELV-Stromkreise angeschloßen werden. Jedoch müssen die bestimmten hierin beschriebenen TNV-Anschlüsse an gleichwertigen Stromkreise angeschloßen werden.

Grounding

This equipment may be equipped with an external grounding nut (#10/32 UNF-2B). For those units requiring grounding, use a grounding wire of No. 18 AWG (.83 mm^2) or greater.

FCC Part 68

This equipment complies with Part 68 of the FCC rules. On the underside of the interface PC board is a label that contains, among other information, the FCC registration number for this equipment. If requested, this information must be provided to the telephone company. (Note: REN [Ringer Equivalence Number] does not apply to this equipment.)

An FCC compliant telephone plug Type RJ48X or RJ48C is provided with this equipment. This equipment is designated to be connected to the telephone network or premises wiring using a compatible modular jack that is Part 68 compliant.

If the T1 terminal equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. If advance notice is not practical, the telephone company will notify the customer as soon as possible. You should be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of this equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

Refer to the following Facility Interface Codes (FICs) when describing the equipment to the telephone company. Choose one of the following and set the software configurable unit to match. Note that password protection is needed to change this feature.

FIC	Description
04DU9-BN	1.544 Mbps Superframe Format (SF) without line power.
04DU9-DN	1.544 Mbps Superframe Format and B8ZS without line power.
04DU9-1KN	1.544 Mbps ANSI Extended Superframe Format (ESF) without line power.
04DU9-1SN	1.544 Mbps ANSI ESF and B8ZS without line power.

Service Order Code

The Service order code for this machine is 6.0F.

TABLE OF CONTENTS

1 INTRODUCTION

A brief overview of the DYNASTAR applications and features.

2 *DYNASTAR* INSTALLATION

An explanation of power, communication line, modem, and network connection requirements for hardware installation for the DYNASTAR.

3 THE SUPERVISOR

A look at menu hierarchies, universal navigation commands, and Supervisor Console connection options.

6 THE X.25 APPLICATION

An explanation of the DYNASTAR X.25 application and of the procedures for implementing all X.25 functions.

7 THE PAD FUNCTION

An explanation of the DYNASTAR asynchronous PAD function and procedures for implementing all PAD functions.

8 THE FRAME RELAY APPLICATION

An explanation of the DYNASTAR frame relay application and procedures for setting up a frame relay connection.

9 ISDN CONFIGURATION

A description of the ISDN configuration and all link parameters.

10 THE PPP APPLICATION

An explanation of how to configure your dedicated and dial PPP calls and how to implement security on a PPP line.

11 THE CSU/DSU MODULE

Capabilities and configuration of the CSU/DSU module.

12 THE IP/IPX ROUTER APPLICATION

How to configure IP and IPX connections through your DYNASTAR, including IPX-In, IPX-Out, and SLIP.

13 TELNET AND ASYNC SERVICES

Examples of how to use Telnet connections and how to configure them in your DYNASTAR.

20 MONITORING AND STATISTICS

An explanation of how to use the status, statistics, monitoring, trace, and log functions.

21 TROUBLESHOOTING

An explanation of some common problems and how to resolve them.

INTRODUCTION

1

APPLICATIONS

The *DYNASTAR* is a multi-service, multi-microprocessor platform that provides a comprehensive set of LAN/WAN solutions and Gateway features for today's networking needs. The unit's hardware and software modules simultaneously support multiple LAN interfaces, WAN interfaces, and LAN/WAN applications.

The *DYNASTAR* units support the following applications and connections:

ROUTER provides IP/IPX/OSI routing between Ethernet LANs over synchronous point-to-point (PPP) lines, X.25, frame relay, ISDN, and ATM networks.

ETHERNET BRIDGE provides, as an Ethernet 802.3 bridge, spanning tree Ethernet-to-Ethernet remote bridging (IEEE 802.1d) over synchronous point-to-point lines or over X.25 or frame relay networks. Manual dial bridge calls are also supported.

X.25 SWITCH AND CONCENTRATOR provides an X.25 DTE access line to an X.25 node and an X.25 DCE interface to support X.25 concentration and switching. It also provides an underlying routing protocol for IPX-In and SLIP services. XOT is also available for carrying X.25 traffic over TCP/IP networks.

X.3, X.28, AND X.29 PAD provides X.3, X.28, and X.29 asynchronous PAD service to terminals, hosts, and modems. These PAD ports also provide access to network elements and alarm management.

FRAME RELAY provides frame relay bridging, routing, and switching. All versions of Links Management Protocol are supported.

ASYNCHRONOUS SERVICES provide multiple gateway functions that support bi-directional services between TCP/IP (Telnet) and async, X.25, IPX, SLIP, and async PPP. This comprehensive suite of Terminal Servers supports 256 concurrent services.

ISDN supports both BRI and PRI WAN/LAN solutions. Each B-channel can be configured to support one of three WAN protocols (PPP, X.25, or frame relay) at transmission speeds of up to 64 kbps. Multilink PPP is available to interleave packets and provide higher throughput.

ATM provides a low-speed Asynchronous Transfer Mode (ATM) access method over T1 or E1 facilities. IP encapsulation overATM, frame relay traffic overATM, X.25 traffic over ATM, and frame relay-to-ATM traffic are supported.

SNA provides support for SNA traffic on the *DYNASTAR*, allowing remote SDLC control units (CUs) to access IBM host computers over X.25 or frame relay networks. Full protocol spoofing and connections between SDLC and LLC2 are supported.

ETHERNET SWITCH provides a 12-position 10Base-T Ethernet switch that can function as an unmanaged Ethernet switch (Ethernet packets are simply passed between ports) or as a managed Ethernet switch. In this latter application, the switch can be partitioned into smaller switches and/or provide additional Ethernet terminal ports that transfer packets internally. The module also supports two 10/100Base-T ports.

OSI.GATE is a separately licensed software application that provides a number of OSI protocol gateway features that provide older legacy managers access to OSI-compliant network elements, allow OSI tunneling through TCP backbones, and give OSI managers control over legacy network elements.

NOTE: For a list of product certifications, see Appendix A.

■ BASE CONFIGURATION

DYNASTAR 100/100i

The *DYNASTAR 100/100i* hardware consists of a *DYNASTAR 100* baseboard installed in a stand-alone chassis. The baseboard has a 25 MHz Motorola 68360 RISC-based processor, 1 Mbyte of RAM (expandable to 16 MB), 2 Mbytes of flash EPROM, a 4 Mbyte SIMM, and 128 kbytes of PROM. Configuration information is written into flash EEPROM.

The *DYNASTAR 100* base configuration consists of:

- One Ethernet LAN port
- Two high-speedWAN ports (V.35 or X.21)
- One synchronous/asynchronous port (V.24/RS-232)
- One asynchronous console port for configuration and diagnostics (V.24/RS-232)

The *DYNASTAR 100i* base configuration provides:

- One ISDN BRI interface (2B + D)
- One Ethernet LAN port
- One high-speed WAN port (V.35 or X.21 or V.24/RS-232)
- One asynchronous console port for configuration and diagnostics (V.24/RS-232)

Expansion slots on both the *DYNASTAR 100* and the *DYNASTAR 100i* provide the capability to support an additional LAN port or multiple WAN or async ports.

Figure 1-1 and Figure 1-2 show the base configuration of the *DYNASTAR 100* and *DYNASTAR 100i* back panels. For more detailed information on hardware and installation, see Chapter 2, *DYNASTAR Installation*.

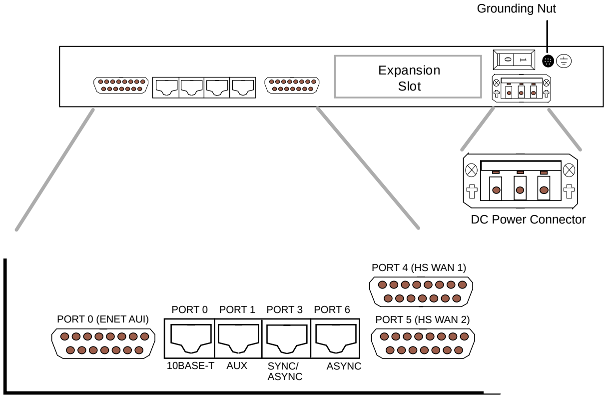


Figure 1-1 ***DYNASTAR 100* Back Panel**

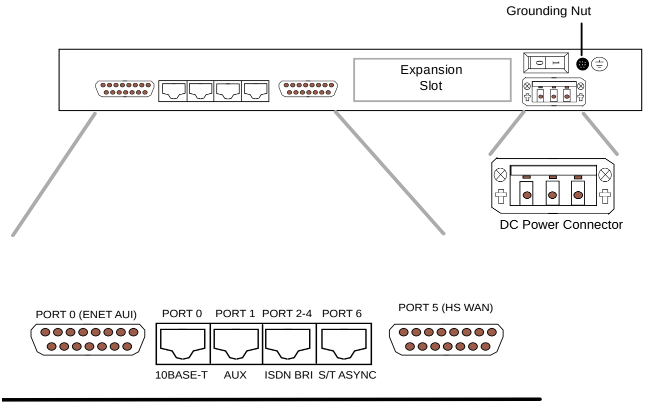


Figure 1-2 ***DYNASTAR 100i* Back Panel**

NOTE: The actual population of your back panel will depend on the options that you have purchased.

PORT NUMBERING. Port use and numbering for the *DYNASTAR 100* is summarized in Table 1-1 and for the *DYNASTAR 100i* in Table 1-2.

Table 1-1 *DYNASTAR 100* Ports

Port Number	Connector	Description
0	AUI or 10BASE-T	On-board Ethernet port
1	AUX or upgraded rear panel DB15 or DB9	ENET interface module port or ATM port, if optional board installed
2	N/A	Reserved
3	Sync/Async V.24/ RS-232	Sync/Async V.24/RS-232 WAN port
4	HS WAN 1	X.21 or V.35 WAN port
5	HS WAN 2	X.21 or V.35 WAN port
6	Async RS-232	Async V.24/RS-232 port (Default port for Supervisor Console)
101-116	Upgraded rear panel	Expansion boards as detailed in *Optional Configurations*

Table 1-2 *DYNASTAR 100i* Ports

Port	Connector	Description
0	AUI or 10BASE-T	On-board Ethernet port
1	AUX or upgraded rear panel DB15 or DB9	ENET interface module port ATM port, if optional board installed
2-4	RJ-45	ISDN S/T interface, 2B+D D=port 2; B1/B2=ports 3 and 4
5	HS WAN	X.21 or V.35 orV.24/RS-232 WAN port

Table 1-2 *DYNASTAR 100i* Ports

Port	Connector	Description
6	Async RS-232	Async V.24/RS-232 port (Default port for Supervisor Console)
101-116	Upgraded rear panel	Expansion boards as detailed in *Optional Configurations*

DYNASTAR 100e

The *DYNASTAR 100e* hardware consists of a *DYNASTAR 100e* baseboard installed in a stand-alone chassis. The baseboard has a 33 MHz Motorola MPC 860 RISC-based processor, 1 Mbyte of RAM (expandable to 16 MB), 2 Mbytes of flash EEPROM, a 16 Mbyte SIMM, and 128 kbytes of PROM. Configuration information is written into flash EEPROM.

The *DYNASTAR 100*e is available in a rack mount chassis only. The *DYNASTAR 100e* base configuration consists of:

- One Ethernet LAN port (10/100 Base-T)
- Two high-speedWAN ports (X.21, V.35, V.24/RS-232, T1/E1, with CSU/DSU, 56k DDS, or MODEM)
- One synchronous/asynchronous port (V.24/RS-232)
- One asynchronous console port for configuration and diagnostics (V.24/RS-232)

NOTE: The base configuration is slightly different if you order the CSU capability.

The two expansion slots on the *DYNASTAR 100e* provide the capability of supporting additional Ethernet,WAN, or serial ports.

The base configuration of the *DYNASTAR 100e* is shown in Figure 1-3. For more detailed information on hardware and installation, see Chapter 2, *DYNASTAR Installation*.

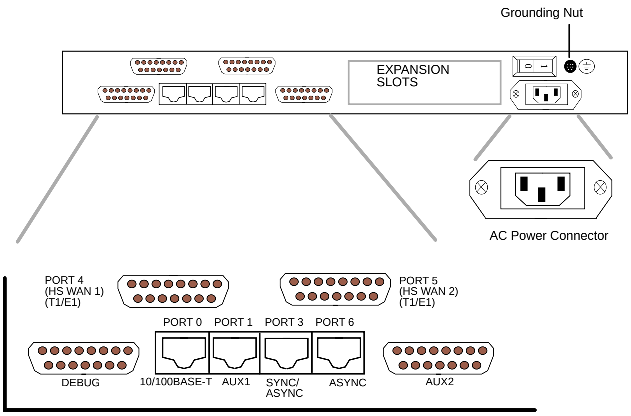


Figure 1-3 *DYNASTAR 100e* Back Panel

NOTE: The actual population of your back panel will depend on the options that you have purchased.

PORT NUMBERING. Port use and numbering for the *DYNASTAR 100e* is summarized inTable 1-3.

Table 1-3 *DYNASTAR 100e* Ports

Port Number	Connector	Description
0	10/100BASE-T	On-board Ethernet port
1	AUX1	ENET interface module port or ATM port, if optional board installed
2	AUX2	ENET interface module port or ATM port, if optional board installed
3	Sync/Async V.24/ RS-232	Sync/Async V.24/RS-232 WAN port
4	HS WAN 1	V.24/RS-232, X.21, V.35, T1/E1, DDS, or Modem WAN port
5	HS WAN 2	V.24/RS-232, X.21, V.35, T1/E1, DDS, or Modem WAN port
6	Async RS-232	Async V.24/RS-232 port (Default port for Supervisor Console)
101-116 201-216	Expansion slots 1 and 2	Expansion modules as detailed in *Optional Configurations*

DYNASTAR 500

The *DYNASTAR 500* hardware consists of a *DYNASTAR 500* baseboard installed in a stand-alone chassis. The baseboard has a 25 MHz Motorola 68360 RISC-based processor, 2 Mbytes of RAM (expandable to 16 MB), and 2 Mbytes of Flash EEPROM, a 4 Mbyte SIMM, and 128 kbytes of PROM. Configuration information is written into Flash EEPROM.

The *DYNASTAR 500* base configuration provides:

- One Ethernet LAN port
- Two high speedWAN ports (X.21, V.35, or V.24/RS-232)
- One synchronous/asynchronous port (V.24/RS-232)
- One asynchronous console port for configuration and diagnostics (V.24/RS-232)

Five expansion slots on the *DYNASTAR 500* provide the capability of supporting three additional Ethernet ports or multiple WAN and async ports.

Figure 1-4 shows the base configuration of the *DYNASTAR 500* back panel. Figure 1-5 shows an enlargement of the bottom row of connectors. For further information on hardware and installation, see Chapter 2, *DYNASTAR Installation*.

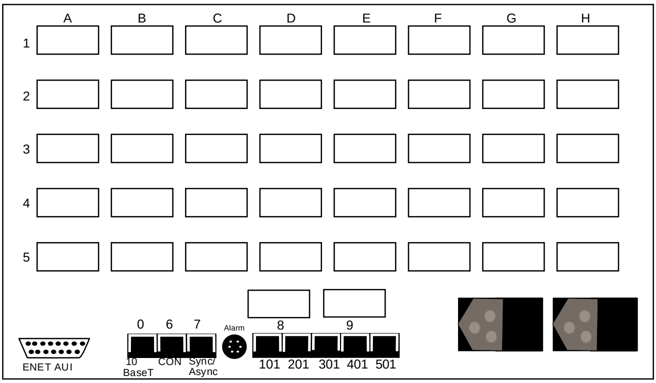


Figure 1-4 *DYNASTAR 500* Back Panel

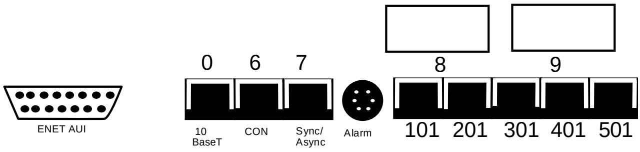


Figure 1-5 Bottom Row of *DYNASTAR 500* Ports

NOTE: The actual population of your back panel will depend on the options that you have purchased.

PORT NUMBERING. The physical ports for the base configuration of the *DYNASTAR 500* are numbered 0 through 9 and 101 through 501 and are shown in Figure 1-4.

Expansion ports are installed in slots 1 through 5, as indicated down the left side of the rear panel. Ports in slot 1 are numbered starting at 101 and continuing in sequence for the number of ports needed. Ports in slot 2 are numbered starting at 201, and so on. The column indications of A through H across the top of the back panel are intended to provide a port referencing scheme for cable installation. For example, port 3D (or D3) is in row 3, column 4 (D). For additional hardware and installation information, please see Chapter 2, *DYNASTAR Installation*.

Port numbering and use are summarized in Table 1-4.

Table 1-4 *DYNASTAR 500* Ports

Port Number	Connector	Description
0	AUI or 10BASE-T	On-board Ethernet port
6	Async V.24/RS-232	Async V.24/RS-232 WAN port (Default port for Supervisor Console)
7	Sync/Async V.24/ RS-232	Sync/Async V.24/RS-232 WAN port
8	HS WAN 1	V.24/RS-232, X.21, V.35, or T1/E1 CSU WAN port
9	HS WAN 2	V.24/RS-232, X.21, V.35, or T1/E1 CSU WAN port
101, 201, 301, 401, 501	Various	Debug/Auxiliary Ports for Slots 1 through 5
101-116 201-216 301-316 401-416 501-516	Expansion Slot 1 Expansion Slot 2 Expansion Slot 3 Expansion Slot 4 Expansion Slot 5	Expansion boards as detailed in *Optional Configurations*

DYNASTAR 2000

The *DYNASTAR 2000* hardware consists of a *DYNASTAR 100e* baseboard installed in a stand-alone 2U high chassis. The baseboard has a 33 MHz Motorola MPC 860 RISC-based processor, 1 Mbyte of RAM (expandable to 16 MB), 2 Mbytes of flash EEPROM, a 16 Mbyte SIMM, and 128 kbytes of PROM. Configuration information is written into flash EEPROM.

The *DYNASTAR 2000* is available in a rack mount chassis only. The *DYNASTAR 2000* base configuration consists of:

- One Ethernet LAN port (10/100 Base-T)
- Two high-speedWAN ports (X.21, V.35, or V.24/RS-232, T1/E1, with CSU/DSU, 56k DDS, or MODEM)
- One synchronous/asynchronous port (V.24/RS-232)
- One asynchronous console port for configuration and diagnostics (V.24/RS-232)

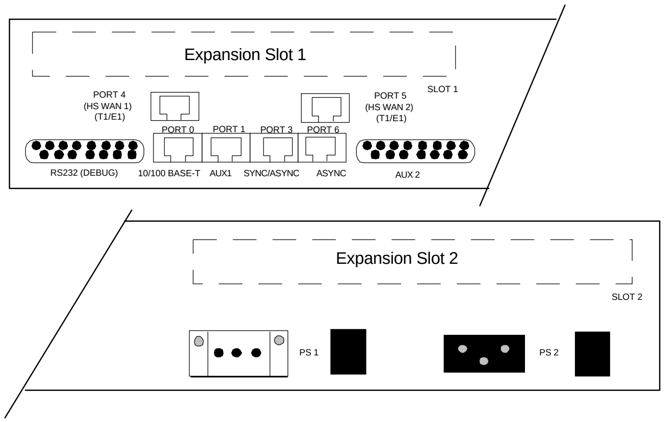
NOTE: The base configuration is slightly different if you order the CSU capability.

Two expansion slots on the *DYNASTAR 2000* provide the capability of supporting additional Ethernet, WAN, or async ports with full utilization of expansion board capability. The *DYNASTAR 2000* also has a relay on the back panel that can be used for power supply failure.

The base configuration of the *DYNASTAR 2000* is shown in Figure 1-6. For more detailed information on hardware and installation, see Chapter 2, *DYNASTAR Installation*.

Figure 1-6 *DYNASTAR 2000* **Back Panel**

NOTE: The actual population of your back panel will depend on the options that you have purchased.



PORT NUMBERING. Port use and numbering for the *DYNASTAR 2000* is summarized in Table 1-5.

Table 1-5 *DYNASTAR 2000* Ports

Port Number	Connector	Description
0	10/100BASE-T	On-board Ethernet port
1	AUX1	ENET interface module port or ATM port, if optional board installed
2	AUX2	ENET interface expansion module port if optional board installed
3	Sync/Async V.24/ RS-232	Sync/Async V.24/RS-232 WAN port
4	HS WAN 1	V.24/RS-232, X.21, V.35, T1/E1, DDS, or Modem WAN port
5	HS WAN 2	V.24/RS-232, X.21, V.35, T1/E1, DDS, or Modem WAN port
6	Async RS-232	Async V.24/RS-232 port (Default port for Supervisor Console)

Table 1-5 *DYNASTAR 2000* Ports (cont.)

Port Number	Connector	Description
101-116	Expansion slot 1	Expansion modules as detailed
201-216	Expansion slot 2	in *Optional Configurations*

DYNASTAR 2000H

The *DYNASTAR 2000H* is a special version of the*DYNASTAR 2000* model that has additional features for use in utility applications. The main features include the following:

- Special surge and pulse withstand power supplies that meet IEEE C37.90.1 standards
- Extended temperature operation (-10° to +65° C)
- Removed fan
- Two available power hardened supplies: 90-250 VAC/DC or 18-60VDC.

The back panel port connections are the same as for the *DYNASTAR 2000*; however, the power supply connection differs and is a screw terminal.

DYNASTAR 5000

The *DYNASTAR 5000* hardware consists of a *DYNASTAR 5000* baseboard installed in a stand-alone chassis. The baseboard has a 50 MHz Motorola MPC860 RISC processor, 16 Mbytes of RAM (expandable to 128 MB), and 4 Mbytes of Flash EEPROM (expandable to 16 Mbytes). Configuration information is written into Flash EEPROM.

The *DYNASTAR 5000* base configuration provides:

- One 10/100 Base-T LAN port (Ethernet)
- Two high speed WAN ports (X.21, V.35, T1/E1, or V.24/RS-232)
- One synchronous/asynchronous port (V.24/RS-232)

- One asynchronous console port for configuration and diagnostics (V.24/RS-232)

Five expansion slots on the *DYNASTAR 5000* provide the capability of supporting additional Ethernet, T1, E1, or ATM ports or multiple WAN and async ports.

The base configuration of the *DYNASTAR 5000* back panel is shown in Figure 1-7. Figure 1-8 shows an enlargement of the bottom row of connectors. For further information on hardware and installation, see Chapter 2, *DYNASTAR Installation*.

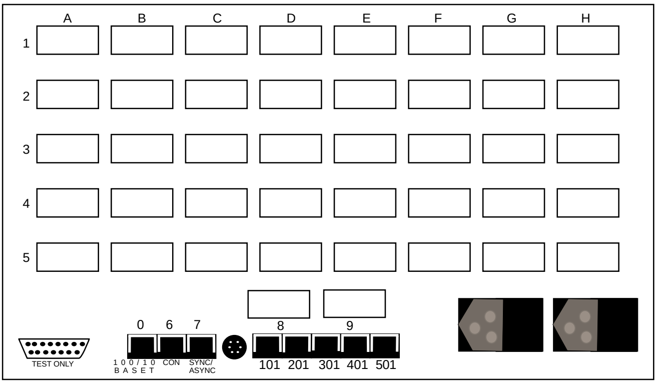


Figure 1-7 ***DYNASTAR 5000* Back Panel**

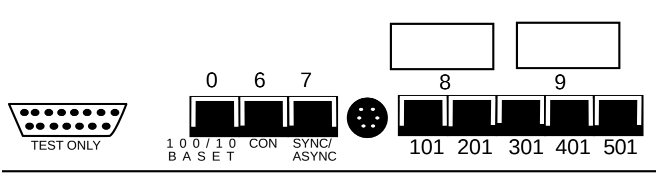


Figure 1-8 **Bottom Row of *DYNASTAR 5000* Ports**

NOTE: The actual population of your back panel will depend on the options that you have purchased.

PORT NUMBERING. The physical ports for the base configuration of the *DYNASTAR 5000* are numbered 0 through 9 and 101 through 501 and are shown in Figure 1-7.

Expansion ports are installed in slots 1 through 5, as indicated down the left side of the rear panel. Ports in slot 1 are numbered starting at 101 and continuing in sequence for the number of ports needed. Ports in slot 2 are numbered starting at 201, and so on. The column indications of A through H across the top of the back panel are intended to provide a port referencing scheme for cable installation. For example, port 3D (or D3) is in row 3, column 4 (D). For additional hardware and installation information, please see Chapter 2, *DYNASTAR Installation*.

Port numbering and use are summarized in Table 1-6.

Table 1-6 *DYNASTAR 5000* Ports

Port Number	Connector	Description
0	10/100BASE-T RJ-45	On-board 10/100 Mbps Ethernet port
6	Async V.24/RS-232	Async V.24/RS-232 WAN port Default port for Supervisor Console (craft port)
7	Sync/Async V.24/ RS-232 RJ-69	Sync/Async V.24/RS-232 WAN port
8	HS WAN 1 DB-15 or RJ-45	V.24/RS-232, X.21, V.35, or T1/E1 WAN port
9	HS WAN 2 DB-15 or RJ-45	V.24/RS-232, X.21, V.35, or T1/E1 WAN port
101, 201, 301, 401, 501	Various	Debug/Auxiliary Ports for Slots 1 through 5
101-116 201-216 301-316 401-416 501-516	Expansion Slot 1 Expansion Slot 2 Expansion Slot 3 Expansion Slot 4 Expansion Slot 5	Expansion boards as detailed in *Optional Configurations*

OPTIONAL CONFIGURATIONS

Interface modules and expansion boards customize the type and number of devices supported. The interface modules available provide physical configurations for a flexible mix of asynchronous, synchronous, ISDN, LAN, Ethernet, TDM, and ATM ports.

Only one expansion board can be installed in a *DYNASTAR 100/100i*. In the rack mount unit, the sync/async expansion ports are to the right of the base configuration ports (Figure 1-1 and Figure 1-2). Two expansion boards can be installed in the *DYNASTAR 100e* and the *DYNASTAR 2000*; however, in the *DYNASTAR 100e* only a limited number of physical ports can be accessed. A maximum of five expansion boards can be installed in slots 1 through 5 of the *DYNASTAR 500* (Figure 1-4) and the *DYNASTAR 5000* (Figure 1-7), depending on the type of board and overall configuration of the unit.

QUAD provides port-by-port flexibility for asynchronous and synchronous interfaces. The QUAD board supports a variety of interfaces, including X.21,V.35, V.24/RS-232, RS-485, and fiber. The QUAD supports speeds up to 115.2 kbps per port via the V.24/RS-232 connector and 256 kbps per port for synchronous X.21 orV.35 with an aggregate throughput of 1 Mbps. Five QUAD boards can be installed in the *DYNASTAR 500* and the *DYNASTAR 5000*.

OCTAL+ provides eight asynchronous ports, each with a V.24/RS-232 interface on an RJ-45 connector. Speed is selectable to 38.4 kbps with an aggregate throughput of 153.6 kbps. (The *DYNASTAR 100e*, *DYNASTAR 2000*, and the *DYNASTAR 5000* do not support the OCTAL+ board.)

8-PORT SYNC/ASYNC provides 8 individually configurable synchronous or asynchronous ports on DB-15 or optical connectors that support X.21, V.35, or V.24/RS-232 operation on a port-by-port basis. The 8-port board operates at speeds up to 230.4 kbps for asynchronous ports, and 256 kbps for synchronous ports (64 kbps for V.24). The 8-port board is configured in the same manner as the QUAD interface module.

16-PORT SYNC/ASYNC provides 16 individually configurable synchronous or asynchronous ports on RJ-69 or optical connectors supporting V.24/RS-232 only. The asynchronous ports support a maximum speed of 115.2 kbps and the synchronous ports, 64 kbps.

ATM provides an ATM interface over T1 or E1 facilities at 1.544 or 2.048 Mbps. This is available only on the two high speed WAN ports on the *DYNASTAR 100e/2000/5000* models.

PRI (T1/E1) provides an ISDN interface over a DS1 connection at 1.544 Mbps (T1) or 2.048 Mbps (E1). It furnishes both primary rate or channelized service, over n x 64 or n x 56 kbps channels. The PRI provides two T1 trunks, two E1 trunks, or one of each, depending on the version you purchase. The board is equipped with two RJ-48 connectors, two DB-15 connectors, two dual coax connectors (E1 only), single-mode or multi-mode optical, or a combination of any two of these connectors. Table 1-7 shows the types of connectors available.

Table 1-7 PRI Connectors

Interface Type	Connectors Available
T1	RJ-48 DB-15 Optical
E1	RJ-48 DB-15 BNC Optical

CHANNELIZED T1/E1, like the PRI interface module, provides a DS1 connection at T1 or E1 speeds. There is no ISDN capability; instead, the bandwidth is divided into n x 64 kbps or (in some cases on a T1 interface) n x 56 kbps channels. The same connector combinations are available for the Channelized T1/E1 card.

BRI provides two ISDN basic rate interfaces, each with two 64 kbps B-channels and one 16 kbps D-channel. The interface module can be configured at the factory as an S/T

interface or a U interface. Both types of interface module are equipped with RJ-48 connectors.

The **CSU/DSU** board gives the *DYNASTAR 100e*, *DYNASTAR 2000*, *DYNASTAR 500*, and the *DYNASTAR 5000* the capability of including an internal T1 or E1 CSU/DSU in the base WAN ports (4/5 or 8/9). The board is available in five configurations: dual T1, dual E1, WAN port plus a single T1, WAN port plus a single E1, or 56/64k DDS with CSU/DSU.

The **CONTACT ALARM AND RELAY** module provides 48 dry contact inputs and 8 controllable relay outputs. The module continuously monitors the inputs and generates TL1 formatted alarm messages or SNMP traps.

The **ETHERNET SWITCH** card provides up to twelve 10BASE-T Ethernet ports and two 10/100Base-T ports for a total of 14 ports. The module can function as an unmanaged switch that simply passes Ethernet packets between ports or as a managed Ethernet switch that can be partitioned into smaller switches and/or provide additional Ethernet terminal ports. The standard ports can be configured with Multi-mode or Single mode optical interfaces supporting the 10FL or 100FX standards.

Several of the expansion boards can be configured with **SINGLE EXPANSION MODULES** that provide a variety of interfaces. The *DYNASTAR* software automatically detects which single expansion modules are installed. This information is passed to the main processor and made available to the operator through the port status screens of the supervisor port. The single expansion modules and the boards that support them are listed below:

- **X.21, V.24/RS-232, and V.35:** supported in any combination on the QUAD expansion module.
- **T1/E1**: supported on the baseWAN ports (ports 4 and 5) on the *DYNASTAR 100e* and the *DYNASTAR 2000* only.
- **DDS**: supported on the base WAN ports (ports 4 and 5) on the *DYNASTAR 100e* and the *DYNASTAR 2000* only.

- **Modem**: An integrated V.90 capable analog modem is available as a base WAN port option (ports 4 and 5) on the *DYNASTAR 100e* and the *DYNASTAR 2000* only.
- **RS-485**: supported on the base WAN ports (4/5 or 8/9) and on the QUAD or 8-port expansion modules.
- **Fiber**: both single mode and multi-mode fiber optic interfaces are supported on a variety of ports, including T1/E1 base WAN ports; the QUAD, 8-port, 16-port, and Ethernet Switch expansion modules; and asynchronous interfaces on base WAN ports on the *DYNASTAR 100e* and the *DYNASTAR 2000/2000H* models.

For information on installing and configuring expansion boards, see Chapter 2, *DYNASTAR Installation*.

■ INTERFACE PROTOCOLS

The interface protocols determine the function of each port, as indicated in this section.

ASYNCHRONOUS

Asynchronous ports can be configured with one of eight asynchronous interface protocols.

IPX-IN supports a NetWare asynchronous IPX connection between a remote workstation and a NetWare LAN.

IPX-OUT supports an asynchronous connection between a NetWare LAN workstation and a distant asynchronous device.

IPX-IN/OUT supports either an IPX-In or IPX-Out call on a dial port.

HDLC provides standard HDLC connections.

SLIP supports incoming asynchronous IP connections.

PAD provides X.3, X.28, and X.29 asynchronous PAD capability.

CONSOLE provides a dedicated port that automatically connects a terminal to the Supervisor.

ASYNC PPP provides point-to-point connection between a work-station and an IP network over either dial-up or direct serial communications lines.

Power utility SCADA protocols allow the *DYNASTAR* to transmit a number of SCADA protocols, including DMP3, PG & E 8971, Modbus, Siemens, and many others.

SYNCHRONOUS

Synchronous ports can be configured with one of four synchronous interface protocols.

X.25 provides X.25 access lines to packet network nodes over X.25 network interfaces. All WAN applications can share the same X.25 access line.

PPP provides point-to-point connection between a pair of LANs for router and bridge applications over PPP synchronous links.

FRAME RELAY provides access lines to frame relay networks for router and bridge applications over frame relay interfaces and provides frame relay switching.

The **MCS-11** transparent protocol is supported on sync/async and baseWAN ports and on the QUAD board. This protocol is the Alcatel microwave SCADA bit-oriented protocol that *DYNASTAR* products can transport over the WAN. This protocol can also be used to transport bit-oriented SCADA protocols like Unitel and PMS91.

■ NETWORK MANAGEMENT

Two kinds of network management are available to the system administrator:

- A built-in, menu-driven Supervisor Console

- An SNMP agent that is accessed from a standard SNMP manager

For more information on the Supervisor, see Chapter 3, *The Supervisor.* For more information on the SNMP capability, see Appendix C.

MIB STRUCTURE

The *DYNASTAR* product MIB is organized under the *DYMEC-DYNASTAR* enterprise 14797 MIB. The MIB definitions for the *DYNASTAR* are available through your service representative.

DYNASTAR INSTALLATION

2

■ WHAT'S IN THE BOX

The shipping package contains:

- The base unit that you have ordered
- One modular cable and adapter for Supervisor port connection to a DTE device (terminal)
- One Ethernet cable (Category Five for UTP connection)
- Power cords as required for your unit
- This user manual on CD
- Warranty and software license

In addition to the baseboard, various expansion modules may already be installed in the unit, depending on what you have ordered.

WARNING: *DYNASTAR* components are comprised primarily of devices sensitive to electrostatic discharge (ESD) and can be damaged if not properly handled. When touching, removing, or replacing any components, disconnect the unit from the power supply and use a grounding wrist strap.

PRE-INSTALLATION

Before installing your *DYNASTAR*, make sure the proper communications network lines are installed at the site. If the *DYNASTAR* is being used as a router or bridge, the site must have at least one Ethernet 10 Mbps or 10/100 Mbps network in place. Depending on the applications supported by your *DYNASTAR*, you may also need dial-in telephone lines, leased lines, a connection to an X.25 PDN, a frame relay connection, and/or a PPP network connection.

To set up the base configuration for the *DYNASTAR*, you need:

- Modems or CSU units.
- Appropriate cables and modular adapters. (Refer to Appendix B for pinout diagrams.)

POWER REQUIREMENTS

Power requirements for the units are given inTable 2-1. A dedicated and surge-protected circuit is recommended but not required. The *DYNASTAR 2000*, *DYNASTAR 500*, and *DYNASTAR 5000* also offer optional dual power supplies for both AC and DC systems.

Table 2-1 Hardware Power Requirements for the *DYNASTAR 100, DYNASTAR 2000, and DYNASTAR 500*

Hardware	Volts	Amps	Watts
DYNASTAR 500	115 VAC 230 VAC 48 DC	0.8 A 0.5 A 0.9 A	42 Watts 44 Watts 35 Watts
DYNASTAR 100/100i Rack mount	115 VAC 230 VAC 48 VDC	0.4 A 0.2 A 0.4 A	22 Watts 22 Watts 18 Watts
DYNASTAR 100e *DYNASTAR 2000*	115 VAC 230 VAC 48 VDC	0.8 A 0.5 A 0.9 A	40 Watts 40 Watts 35 Watts
DYNASTAR 2000H	90-250 VAC/DC 18-60 VDC		30 Watts 30 Watts

Table 2-1 Hardware Power Requirements for the *DYNASTAR 100, DYNASTAR 2000, and DYNASTAR 500*

Hardware	Volts	Amps	Watts
Expansion Modules			3.0 - 4.0 Watts per module installed

.

Table 2-2 Hardware Power Requirements for the *DYNASTAR 5000*

Hardware	Volts	Minimum Watts	Maximum Watts
DYNASTAR 5000	115 VAC 230 VAC 48 DC	50 Watts 50 Watts 50 Watts	220 Watts 220 Watts 220 Watts
Expansion Modules			5.5 Watts per module installed

ETHERNET LAN REQUIREMENTS

The *DYNASTAR* is connected to a LAN using standard cable connections (10BASE-T or AUI; 100BASE-T for the *DYNASTAR 100e*, *DYNASTAR 2000*, and *DYNASTAR 5000*). Verify that the necessary wire or cable is installed at your site.

If the *DYNASTAR* is to support any NetWare related applications, the LAN must have NetWare 286V2.x, 386V3.x, or 486V4.x installed.

NOTE: The *DYNASTAR* can act as a server if a NetWare file server is not present.

Synchronous Line Requirements

Synchronous modems are frequently used on synchronous PPP, X.25, SDLC, and frame relay ports. To meet minimum requirements, modems operating as DCEs must:

- Support full-duplex data transfer.
- Provide both transmit and receive clock.
- Provide constant carrier (i.e., not require Request To Send [RTS] from the *DynaStar*).
- Set Data Carrier Detect (DCD).
- Require only one input data set signal. (The unit uses Data Terminal Ready [DTR].)

X.25 and PPP dial ports support both Hayes AT command compatible and V.25bis (HDLC version) modems.

Asynchronous Line and Modem Requirements

Asynchronous modems are used for dial and leased line connections between the *DynaStar* and remote workstations and/or distant asynchronous devices.

To support asynchronous applications, a leased line modem (or line driver) must:

- Provide full-duplex data transfer
- Support 8-bit transparent data
- Output the Data Carrier Detect (DCD) data set signal

Asynchronous ports can be configured to have dial-in and/or dial-out access. The *DynaStar* uses Hayes-compatible modems. Three standards are supported:

- V.22bis for 2400 baud and lower
- V.32 and V.32bis for 19,200 baud and lower
- V.Fast for 28,800 baud and lower

Dialed lines require one or more rotaries of numbers for incoming calls and, if you plan to provide dial-up access to the console port, one telephone line for the console.

ISDN Requirements

The *DYNASTAR 100i* includes an integral TA (Terminal Adapter) presenting an S/T interface. This requires an external NT-1 unit that should normally be provided by your local carrier.

■ Rack Installation

All *DYNASTAR* units are 19-inch rack mountable. Observe the precautions listed below when rack mounting your *DYNASTAR*:

- If the *DYNASTAR* is installed in a closed or multi-unit rack assembly, the operating ambient temperature may be greater than room ambient temperature. Make sure the *DYNASTAR* is installed in an environment that does not exceed the *DYNASTAR*'s maximum rated ambient temperature, which is 65°C.
- Be sure that there is sufficient air flow for safe operation of the equipment.
- Mount the equipment in the rack so that hazardous conditions (such as top-heavy loading) are avoided.
- Be sure that rack-mounted equipment is reliably grounded. Use the ground nut(s) that is (are) provided on the rear panel. In addition, pay particular attention to supply connections, such as power strips, that are not direct connections to the branch circuit.

*DYNASTAR 100/**100i/100e/2000/2000H*** Rack Mount Mounting Positions

The *DYNASTAR 100*, *DYNASTAR 100e*, *DYNASTAR 100i* and the *DYNASTAR 2000* are mounted using the set of mounting brackets provided with the unit. The unit can be mounted flush with the rack, mounted mid-rack, or wall mounted as shown in Figure 2-1.

NOTE: When wall mounted, the front of the unit must be installed facing upward.

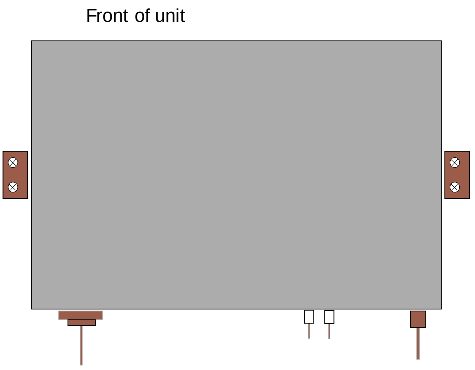
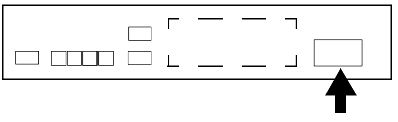


Figure 2-1 Wall Mounted Unit

■ POWER CONNECTIONS

.

CONNECTING THE POWER SUPPLY (*DYNASTAR 100)*



AC POWER, *DYNASTAR 100/100i/100e.*

The AC version of the *DYNASTAR 100/100i/100e* has a single power supply. The AC powered unit operates between 100 and 240 Volts AC with a current of 1 Amp. The power cable mates with a standard EIA 320 connector on the *DYNASTAR*.

CAUTION: Refer to nameplate ratings to be sure that you are not overloading existing circuits when you are connecting your *DYNASTAR*. Overloading could adversely affect overcurrent protection and supply wiring. If in doubt, consult a qualified electrician.

1. Insert the *DYNASTAR* into the rack opening until the mounting ears contact the mounting rails of the rack.

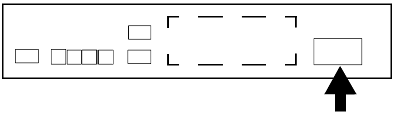
Align the holes in the mounting ears with those in the rails and secure the switch to the rack with the appropriate hardware (such as self-tapping or machine screws and washers).

2. Connect the power cord to the power connection on the *DYNASTAR* rear panel and plug the other end into an appropriate outlet.

3. Power on the unit by turning on the switch on the back of the unit.

NOTE: For added safety, a number 10 ground stud is provided for connection to a separate grounding system. Refer to local codes for installation.

DYNASTAR 100
(DC POWER UNIT)



DC POWER, *DYNASTAR 100/100i/100e.*

The DC-powered *DYNASTAR 100*, *DYNASTAR 100i*, and *DYNASTAR 100e* operate between 42 and 56 Volts with a current of 1.5 Amps. The DC unit is accompanied by a special connector to be installed on your power cable and inserted as illustrated in Figure 2-2. Use 12 to 18 gauge(AWG) wire for the cable.

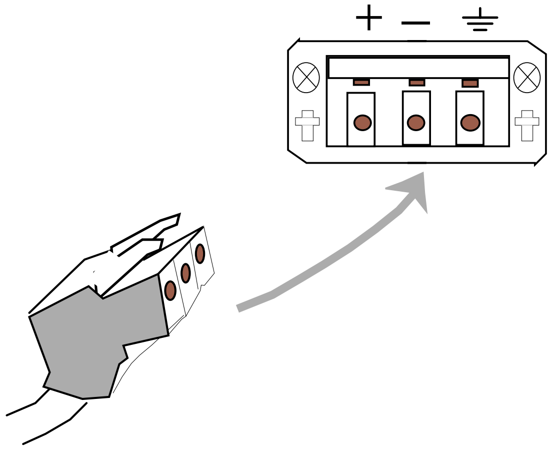


Figure 2-2 DC Power Plug and Mating Connector

If your *DYNASTAR 100* is a DC-powered system, install the unit as follows:

1. Insert the *DYNASTAR* into the rack opening until the mounting ears contact the mounting rails of the rack. Align the holes in the mounting ears with those in the rails and secure the switch to the rack with the appropriate hardware (such as self-tapping or machine screws and washers).

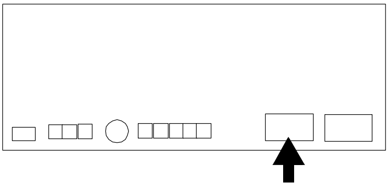
2. Connect the unit to a 48-volt DC source that is electrically isolated from the AC source and that is reliably connected to ground.

   NOTE: For added safety, a number 10 ground stud is provided for connection to a separate grounding system. Refer to local codes for installation.

3. Power on the unit by turning on the switch on the rear panel.

DYNASTAR 500 UNITS

CONNECTING THE POWER SUPPLY (*DYNASTAR 500*)



AC POWER, *DYNASTAR 500*.

The *DYNASTAR 500* offers optional dual power supplies for AC systems. The connection for the main power supply is the innermost of the two connectors on the rear panel (indicated by the arrow in the diagram above), and the redundant power connection is to its right. If you have a *DYNASTAR 500* with redundant power supplies, place the unit in a location with two independent power outlets of the appropriate voltage. To gain the benefit of the dual redundant power system, these power sources should be completely independent and independently fused.

CAUTION: When connecting your *DYNASTAR 500*, refer to nameplate ratings to be sure that you are not overloading existing circuits. Overloading could adversely affect overcurrent protection and supply wiring. If in doubt, consult a qualified electrician.

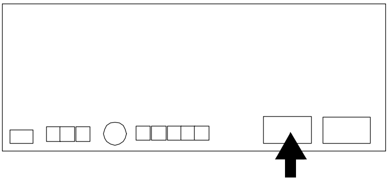
1. If you are rack mounting the unit, insert the *DYNASTAR 500* into the rack opening until the mounting ears contact the mounting rails of the rack. Align the holes in the mounting ears with those in the rails and secure the switch to the rack with the appropriate hardware (such as self-tapping or machine screws and washers).

2. Connect the power cord to the power connection marked PSU1 on the *DYNASTAR 500* rear panel and plug the other end into an appropriate outlet.

3. If you have purchased the redundant power option, plug the second power cord into the remaining power connection and plug the other end into an AC outlet.

4. Power on the unit by opening the front panel and turning on the switch on the internal power unit.

DYNASTAR 500
(DC POWER UNIT)



DC POWER, *DYNASTAR 500*.

The *DYNASTAR 500* offers optional dual power supplies for DC systems. The connection for the main power supply is the innermost of the two connectors on the rear panel (indicated by the arrow in the diagram above), and the redundant power connection is to its right. If you have a *DYNASTAR 500* with redundant power supplies, place the unit in a location with two independent power outlets of the appropriate voltage. To gain the benefit of the dual redundant power system, these power sources should be completely independent and independently fused.

CAUTION: When connecting your *DYNASTAR 500*, refer to nameplate ratings to be sure that you are not overloading existing circuits. Overloading could adversely affect overcurrent protection and supply wiring. If in doubt, consult a qualified electrician.

1. If you are rack mounting the unit, insert the *DYNASTAR 500* into the rack opening until the mounting ears contact the mounting rails of the rack. Align the holes in the mounting ears with those in the rails and secure the switch to the rack with the appropriate hardware (such as self-tapping or machine screws and washers).

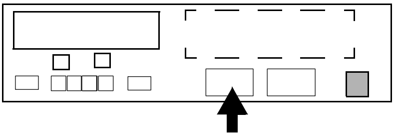
2. Connect the power cord to the power connection marked PSU1 on the *DYNASTAR 500* rear panel and connect the other end to a 48-volt DC source.

3. If you have purchased the redundant power option, plug the second power cord into the remaining power connection and plug the other end into another DC source.

4. Power on the unit by opening the front panel and turning on the switch on the internal power unit.

DYNASTAR 2000 UNITS

CONNECTING THE POWER SUPPLY (*DYNASTAR 2000*)



AC POWER, *DYNASTAR 2000*.

The AC version of the *DYNASTAR 2000* offers optional dual power supplies. The connection for the main power supply is the innermost of the two connectors on the rear panel (indicated by the arrow in the diagram above), and the redundant power connection is to its right. If you have a *DYNASTAR 2000* with redundant power supplies, place the unit in a location with two independent power outlets of the appropriate voltage. To gain the benefit of the dual redundant power system, these power sources should be completely independent and independently fused.

CAUTION: Refer to nameplate ratings to be sure that you are not overloading existing circuits when you are connecting your *DYNASTAR*. Overloading could adversely affect overcurrent protection and supply wiring. If in doubt, consult a qualified electrician.

1. Insert the *DYNASTAR* rack mount into the rack opening until the mounting ears contact the mounting rails of the rack. Align the holes in the mounting ears with those in the rails and secure the switch to the rack with the appropriate hardware (such as self-tapping or machine screws and washers).

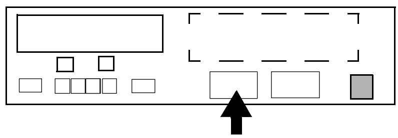
2. Connect the power cord to the main power connection on the *DYNASTAR* rear panel and plug the other end into an appropriate outlet.

3. If you have purchased the redundant power option, plug the second power cord into the remaining power connection and plug the other end into an AC outlet.

4. Power on the unit by turning on the switch on the back of the unit.

   NOTE: For added safety, a number 10 ground stud is provided for connection to a separate grounding system. Refer to local codes for installation.

DYNASTAR 2000
(DC POWER UNIT)



DC POWER, *DYNASTAR 2000*.

The DC-powered *DYNASTAR 2000* operates between 42 and 56 Volts with a current of 1.5 Amps. The DC unit is accompanied by a special connector to be installed on your power cable and inserted as illustrated in Figure 2-2. Use 12 to 18 gauge (AWG) wire for the cable.

The DC version of the *DYNASTAR 2000* offers optional dual power supplies. The connection for the main power supply is the innermost of the two connectors on the rear panel (indicated by the arrow in the diagram above), and the redundant power connection is to its right. If you have a *DYNASTAR 2000* with redundant power supplies, place the unit in a location with two independent power outlets of the appropriate voltage. To gain the benefit of the dual redundant power system, these power sources should be completely independent and independently fused.

1. If you are rack mounting the unit, insert the *DYNASTAR 2000* into the rack opening until the mounting ears contact the mounting rails of the rack. Align the holes in the mounting ears with those in the rails and secure the switch to the rack with the appropriate hardware (such as self-tapping or machine screws and washers).

2. Connect the power cord to the main power connection on the *DynaStar 2000* rear panel and connect the other end to a 48-volt DC source.

   NOTE: For added safety, a number 10 ground stud is provided for connection to a separate grounding system. Refer to local codes for installation.

3. If you have purchased the redundant power option, plug the second power cord into the remaining power connection and plug the other end into another DC source.

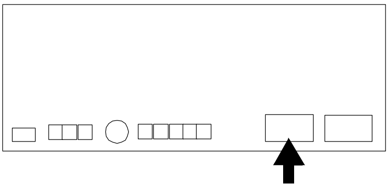
4. Power on the unit by turning on the switch on the rear panel.

DC Power, *DynaStar 2000H*.

The *DynaStar 2000H* offers a special power supply for the utility industry. This power supply is located on the rear of the unit on the right-hand side. It is a screw-down terminal with two screws.

DynaStar 5000 Power Connections

Connecting the Power Supply (*DynaStar 5000*)



AC Power. The *DynaStar 5000* offers optional dual power supplies for AC systems. The connection for the main power supply is the innermost of the two connectors on the rear panel (indicated by the arrow in the diagram above), and the redundant power connection is to its right. If you have a *DynaStar 5000* with redundant power supplies, place the unit in a location with two independent power outlets of the appropriate voltage. To gain the benefit of the dual redundant

power system, these power sources should be completely independent and independently fused.

CAUTION: When connecting your *DYNASTAR 5000*, refer to nameplate ratings to be sure that you are not overloading existing circuits. Overloading could adversely affect overcurrent protection and supply wiring. If in doubt, consult a qualified electrician.

1. If you are rack mounting the unit, insert the *DYNASTAR 5000* into the rack opening until the mounting ears contact the mounting rails of the rack. Align the holes in the mounting ears with those in the rails and secure the switch to the rack with the appropriate hardware (such as self-tapping or machine screws and washers).
2. Connect the power cord to the power connection marked PSU1 on the *DYNASTAR 5000* rear panel and plug the other end into an appropriate outlet.
3. If you have purchased the redundant power option, plug the second power cord into the remaining power connection and plug the other end into an AC outlet.
4. Power on the unit by opening the front panel and turning on the switch on the internal power unit.

DC POWER. The *DYNASTAR 5000* offers optional dual power supplies for DC systems. The connection for the main power supply is the innermost of the two connectors on the rear panel (indicated by the arrow in the previous diagram), and the redundant power connection is to its right. If you have a *DYNASTAR 5000* with redundant power supplies, place the unit in a location with two independent power outlets of the appropriate voltage. To gain the benefit of the dual redundant power system, these power sources should be completely independent and independently fused.

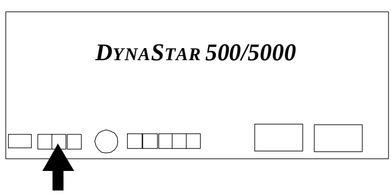
CAUTION: When connecting your *DYNASTAR 5000*, refer to nameplate ratings to be sure that you are not overloading existing circuits. Overloading could adversely affect overcurrent protection

and supply wiring. If in doubt, consult a qualified electrician.

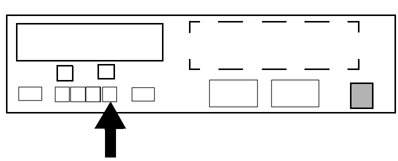
1. If you are rack mounting the unit, insert the *DYNASTAR 5000* into the rack opening until the mounting ears contact the mounting rails of the rack. Align the holes in the mounting ears with those in the rails and secure the switch to the rack with the appropriate hardware (such as self-tapping or machine screws and washers).
2. Connect the power cord to the power connection marked PSU1 on the *DYNASTAR 5000* rear panel and connect the other end to a 48-volt DC source.
3. If you have purchased the redundant power option, plug the second power cord into the remaining power connection and plug the other end into another DC source.
4. Power on the unit by opening the front panel and turning on the switch on the internal power unit.

SUPERVISOR CONSOLE

CONNECTING THE SUPERVISOR CONSOLE



DYNASTAR 2000 (100 is similar)



To set the configuration parameters for the *DYNASTAR*, you need a Supervisor Console. The Supervisor Console must be an asynchronous display that generates and responds to a subset of cursor movement codes that are compatible with either the WYSE 50 and TeleVideo 910, 920, or 925, or with

those defined for a personal computer running in a terminal emulation mode (ANSI or VT100 compatible).

Port 6 on the *DYNASTAR* models is preconfigured as the asynchronous console port. On the *DYNASTAR 100* and *2000* models, this port is labeled *ASYNC*. On the *DYNASTAR 500* and *5000*, it is labeled *CON*. To connect the Supervisor Console to the console port:

1. Plug one end of the supplied modular cable into Port 6.
2. Plug the other end into the supplied DB-9 or DB-25 adapter.
3. Plug the adapter into the asynchronous terminal.
4. Set the communication parameters on the asynchronous terminal to 9600 bps and even parity (7 bits, even, 1 stop).
5. To log in to the Supervisor port, see Chapter 3, *The Supervisor*.

NOTE: After the *DYNASTAR* has been installed and tested, a workstation or a remote terminal can be used as the Supervisor Console. Port 6 can then be reconfigured for other applications.

RUNNING POWER-ON TESTS

When the *DYNASTAR* is turned on, power-on self tests are performed. These tests are indicated on the *DYNASTAR 100* models and the *DYNASTAR 2000* by certain LED patterns, and messages are displayed on the console. The messages displayed during a successful test on the *DYNASTAR 100/100i* are shown in Figure 2-3. Similar messages appear on the other *DYNASTAR* consoles; however, on the *DYNASTAR 500* and the *DYNASTAR 5000*, the front panel LEDs do not display a test pattern.

If any serious power-on tests fail, an error message is displayed in the start-up text on your screen. (At the end of a normal power-on, the entire error log is displayed.) Rerun the tests by powering off your *DYNASTAR* and powering it on again. If the tests fail again, contact your service representative.

```
DYMEC-Dynastar, Inc.
Flash 0 is 1 MB Intel [ID=xxxx]
Flash 1 is 1 MB Intel [ID=xxxx]
DynaStar 100i ROM version x.x
Serial number 399c
Ethernet address xxxxxxxxxxxx
*** Press ESC to boot download.bin immediately ***
*** Press CR to enter LAN monitoring mode ***
Test 128k ROM
Test 16 MB RAM addresses
Test 16 MB RAM pattern
Test 1 MB flashes
Monitoring LAN for ROM commands
Get IP address from SRAM copy #2 of 2
Current IP Address is xxx.xxx.xxx.xxx
Enter different IP Address:
Loading Download.BIN

*****************Error Log******************
```

Figure 2-3 *DYNASTAR 100/100i* Power-on Self Test Messages

FRONT PANEL LEDS

After the power-on tests have been run, the front panel LEDs light to indicate the status of the ports. There is a single LED per port in the *DYNASTAR 100*/*100i*, as shown in Figure 2-4. The *DYNASTAR 100e* is similar, but is not illustrated. The meaning of these LEDs is given in Table 2-3.

DYNASTAR 100e

DYNASTAR 100i

Figure 2-4 Example of *DYNASTAR 100* Front Panels

Table 2-3 *DYNASTAR 100/100i/100e/ 2000/2000H* LEDs

Port	Color and Meaning
Ethernet (Port 0)	Green: Link up Amber: No connection Red: Port disabled
Aux (Port 1) Aux (Port 2)	Off: No daughterboard installed Amber: No call up on any port (for asynchronous transmissions) or no link layer up (for synchronous transmissions) Green: Call up on at least one port (for asynchronous transmissions) or DSS present on at least one port (for synchronous transmissions) **If T1/E1 installed** Red: All trunks disabled Amber: At least one trunk enabled with no trunks up Green: At least one trunk up with no alarms Flashing red: Daughterboard failure If Contact module installed Red: One or more inputs in alarm Green: All inputs normal
ISDN D (ISDN ports are 2-4 on *DYNASTAR 100i* only.)	Amber: No call up Green: Valid connection Red: Port disabled
ISDN B1 and ISDN B2 (ISDN ports are 2-4 on *DYNASTAR 100i* only.)	Blinking amber-green: Call being established Green: Call up Amber: No call up
Sync/Async	Green: Link up Red and green: DSS not present Both red: Port disabled

Table 2-3 *DYNASTAR 100/100i/100e/ 2000/2000H* LEDs (cont.)

Port	Color and Meaning
HS WAN 1 HS WAN 2	**Synchronous** Green: Link up Red and green: DSS not present Both red: Port disabled **Asynchronous** Both green: Call up Red and green: Call down Both red: Port disabled **CSU** Red: Trunk disabled Amber: Trunk enabled but status is down Green: Trunk up with no alarms
Async (Port 6, typically Console)	Amber: No call up Green: Call up
System	Amber: Reboot initiated Green: Powered on

On the *DYNASTAR 500* and the *DYNASTAR 5000*, two LEDs correspond to each port (Figure 2-5). The meaning of these LEDs is given in Table 2-4.

Figure 2-5 *DYNASTAR 500/5000* Front Panel

The *DYNASTAR 500* and the *DYNASTAR 5000* also have alarm and power system LEDs located on the bottom right of the front panel. To the left of these LEDs are three pushbuttons

that are used to test the audible power supply alarms (PS1 Alm Test and PS2 Alm Test) and disable the audible alarm once it has been activated (Alarm Inhibit). These LED indications are explained in Table 2-5.

Table 2-4 *DYNASTAR 500/5000* LEDs

Port Type or Interface Module	LED Color and Meaning
Ethernet (Port 0)	Green: Link up Amber: No connection Red: Port disabled
Console (Port 6)	Amber: Reboot initiated Green: Powered on
Async/Sync (Port 7)	**Synchronous *** Green: Link up Red/green: DSS not present Both red: Port disabled **Asynchronous *** Both green: Call up Red/green: Call down Both red: Port disabled
HS WAN1 and HS WAN2 (Ports 8 & 9)	**Synchronous** Green: Link up Red/green: DSS not present Both red: Port disabled **Asynchronous** Both green: Call up Red/green: Call down Both red: Port disabled
OCTAL+ (*DYNASTAR 500* only)	Both green: Call up Red/green: Call down Both red: Port disabled Blinking red: Daughterboard failure
QUAD	**Synchronous** Green: Link up Red/green: DSS not present Both red: Port disabled **Asynchronous** Both green: Call up Red/green: Call down Both red: Port disabled

Table 2-4 *DYNASTAR 500/5000* LEDs (cont.)

Port Type or Interface Module	LED Color and Meaning
ENET	Green: Link up Amber: No connection Red: Port disabled
16-PORT SYNC/ASYNC **	**Synchronous** Green: Link up Red/green: DSS not present Red: Port disabled Flashing red: Daughterboard failure **Asynchronous** Green: Call up Red/green: Call down Red: Port disabled Flashing red: Daughterboard failure
8-PORT SYNC/ASYNC	**Synchronous** Green: Link up Red/green: DSS not present Both red: Port disabled Flashing red: Daughterboard failure **Asynchronous** Both green: Call up Red/green: Call down Both red: Port disabled Flashing red: Daughterboard failure
ATM	Both red: The trunk is disabled. Red/green: Trunk enabled, but there is an alarm. Both green: The trunk is up with no alarms. Flashing red: Daughterboard failure
T1/E1	Both red: The trunk is disabled. Red/green: The trunk is enabled, but there is an alarm. Or for PRI, the D-channel is not up. Both green: Trunk is up with no alarms. For PRI, the trunk and the D-channel are up with no alarms. Flashing red: Daughterboard failure
BRI	Both red: The trunk is disabled. Red/green: The trunk is enabled, but there is an alarm. Both green: The trunk is up with no alarms. Flashing red: Daughterboard failure

Table 2-4 *DYNASTAR 500/5000* LEDs (cont.)

Port Type or Interface Module	LED Color and Meaning
Contact	Left LED: Red: one or more inputs in ALARM Green: no inputs in ALARM Off: disabled/interface missing Right LED: Red: Alarm output ACTIVE Green: Alarm output INACTIVE Flashing Red: daughterboard failure
Ethernet Switch	One LED per port Amber: link down Green: link up Red: port disabled Off: no port available

* Synchronous transmissions: X.25, frame relay, PPP
Asynchronous transmissions: PAD, Async PPP, SDLC, SLIP, IPX-In, IPX-Out, IPX-In/Out, Console

** For the 16-port card, the two LEDs per port are in a single slot, one above the other. The top LED acts like the left-hand LED, and the bottom like the right-hand LED.

Table 2-5 Power Supply and Alarm LED s

LED	Meaning
PS1 and PS2	Off = monitoring disabled Green = normal Red = failed
ALARM	Red = a power supply or temperature alarm has occurred
OVER TEMP	Off = monitoring disabled Green = temperature normal Amber = temperature too low (below 5° C) Red = temperature too high (above 45° C)
PS1 ALM TEST PS2 ALM TEST	Push to test the alarm for Power Supply 1 or 2. (Sends SNMP audible and operates relay contact alarms.)
ALARM INHIBIT	Push to cancel audible alarm. (Alarm LED will keep blinking.)

On the rear of the *DYNASTAR 500* and *DYNASTAR 5000* chassis, there is also an external alarm output located between ports 7 and 101 that can be connected to an external device. (Refer to Appendix B for pinout information.)

NOTE: The *DYNASTAR 500* and *DYNASTAR 5000* power supply and alarm LEDs can be disabled from the Applications menu.

■ BOARD CONFIGURATION AND INSTALLATION

Your *DYNASTAR* unit is delivered to you fully assembled with the hardware configuration that you ordered, so you will not need to configure or install any boards. However, if at some later date you need to modify your hardware, this section explains how to install and configure all boards that can be added to your *DYNASTAR*.

WARNING: Only qualified service personnel should remove the *DYNASTAR*'s cover, install or replace boards, or modify jumper settings.

DYNASTAR 100 BASEBOARD

As shown in Figure 2-6, there are several sets of jumper blocks on the *DYNASTAR 100* baseboard: the CLR/CONFIG jumper, the HS WAN port operation jumpers, the V.35 grounding jumpers, and the JP14 and JP15 grounding jumpers.

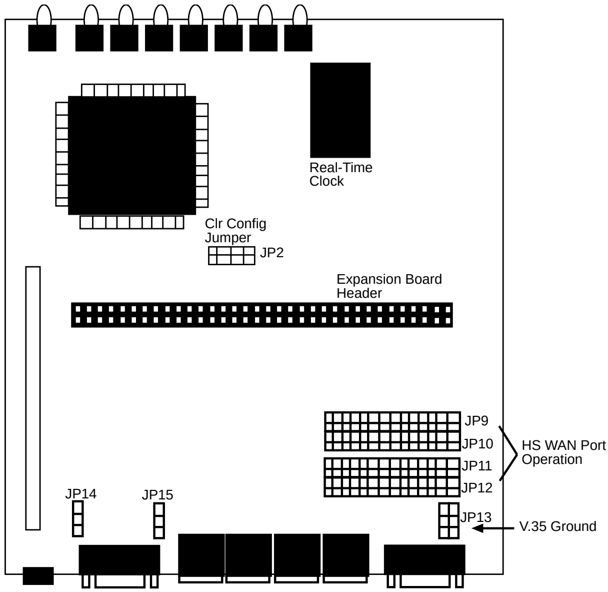


Figure 2-6 ***DYNASTAR 100* Baseboard**

DYNASTAR 100i BASEBOARD

As shown in Figure 2-7, the jumpers on the *DYNASTAR 100i* vary somewhat from those on the *DYNASTAR 100*. The *DYNASTAR 100i* has an additional set of jumpers for resistor termination, and the HS WAN port operation jumpers are different. These variations are described in the sub-sections that follow.

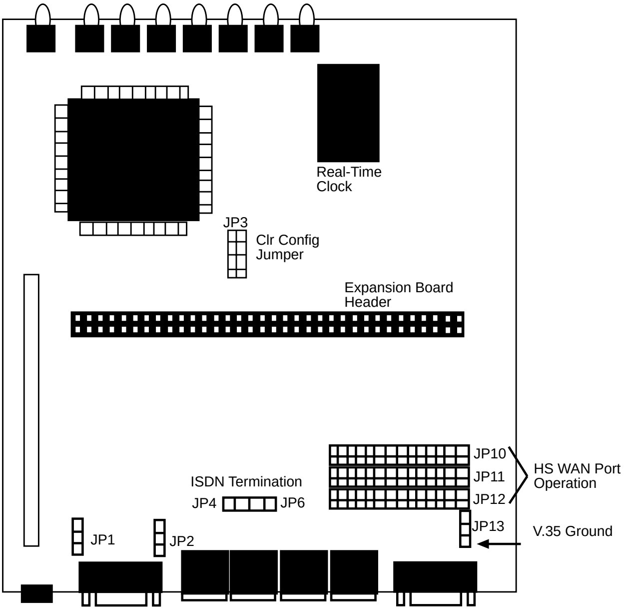


Figure 2-7 ***DYNASTAR 100i* Baseboard**

DYNASTAR 100e AND *DYNASTAR 2000/2000H* BASEBOARD

The *DYNASTAR 100e* and *DYNASTAR 2000/2000H* baseboard is shown in Figure 2-8. Like the *DYNASTAR 100* and *DYNASTAR 100i*, this baseboard has a clear configuration jumper. Unlike the other boards, the *DYNASTAR 100e/ DYNASTAR 2000/2000H* has no WAN port operation jumpers but does have a reset button, an additional expansion board header, and port bias jumpers.

CLEAR CONFIGURATION JUMPER. A 4 x 2 pin jumper block is located in the center of the board on the *DYNASTAR 100* (JP2) and the *DYNASTAR 100i* (JP3). The jumper is shown in the baseboard diagrams (Figure 2-6 and Figure 2-7) and is shown enlarged in Figure 2-9. On the *DYNASTAR 100e* and *DYNASTAR 2000/2000H*, the 2-pin Clr Config jumper is located at the edge of the board near the LEDs (Figure 2-8). The Clr Config pin pair can be used to force all configuration parameters to revert to default values.

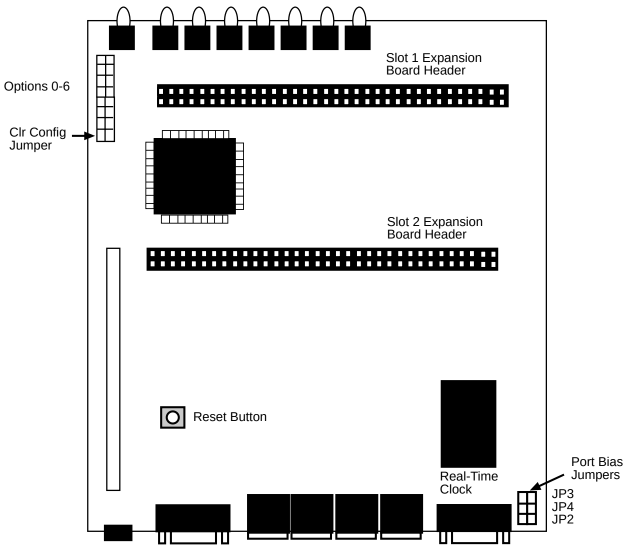


Figure 2-8 *DYNASTAR 100*e Baseboard

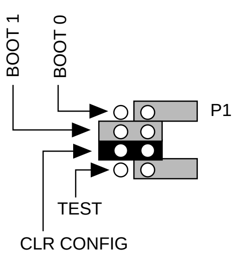


Figure 2-9 Clear Configuration Jumper (*100/100i*)

To clear configuration parameter values:

1. Power down the *DYNASTAR*.
2. Unscrew the baseboard from the rear of the chassis and slide it out.
3. Remove the CLR CONFIG shunt.
4. Power up the *DYNASTAR* with the shunt removed.
5. After the unit has booted, install the shunt again, leaving the *DYNASTAR* on.

✓ All factory settings revert to the factory defaults.

NOTE: Only the CLR/CONFIG shunt should be removed. The other shunts in the jumper block are used during board manufacture and should not be changed.

HS WAN PORT OPERATION. Behind the HS WAN ports on the *DYNASTAR 100* are four 14 x 2 pin jumper blocks (JP9 - JP12) that are used to specify the use of X.21 or V.35 for HS WAN ports 4 and 5 (shown in Figure 2-6 and enlarged in Figure 2-10).

On the *DYNASTAR 100i*, there are three 14 x 2 pin jumper blocks to specify use of X.21, V.35, or V.24 for HS WAN port 5 (shown in Figure 2-7 and enlarged in Figure 2-11).

BABT units are shipped with a default setting of X.21 operation (BABT units can be identified by the marking *CE168* on the bottom of the unit). Other units are shipped with a default setting of V.35 operation. To modify the setting, remove the shunts and place them over the desired row of pins, as indicated by the silkscreen.

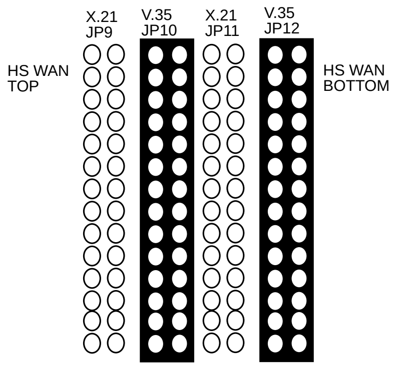


Figure 2-10 ***DynaStar 100*** **WAN Port Operation Jumpers Showing V.35 Selection**

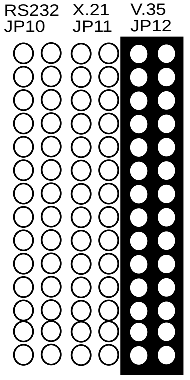


Figure 2-11 ***DynaStar 100i*** **WAN Port Operation Jumpers Showing V.35 Selection**

GROUND FOR V.35 OPERATION. On the *DYNASTAR 100*, there is a 2 x 3 pin jumper block (JP13) located next to the X.21/V.35 jumpers (Figure 2-6; enlarged in Figure 2-12). This jumper block lets you specify whether Pin 1 of the DB-15 connector for the associated V.35 WAN port is connected to signal ground or chassis ground. By default (as shown in Figure 2-12) both ports are connected to chassis ground.

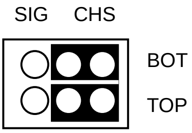


Figure 2-12 *DYNASTAR 100* V.35 Grounding Pins

On the *DYNASTAR 100i*, there is a single 1 x 3 pin jumper block (JP13) to the right of the RS-232/X.21/V.35 jumper block (Figure 2-7 and enlarged in Figure 2-13). This 1 x 3 pin jumper block lets you specify whether Pin 1 of the DB-15 connector for port 5 is connected to signal ground or chassis ground for V.35. Place the shunt over the two left-hand pins to indicate signal ground or over the two right-hand pins to indicate chassis ground. Chassis ground is the default.

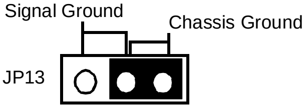


Figure 2-13 *DYNASTAR 100i* V.35 Grounding Pins

ISDN TERMINATION. Two 1 x 2 pin jumper blocks, labeled JP4 and JP6, are located behind the RJ-45 connector for the ISDN interface on the *DYNASTAR 100i* (see location in Figure 2-7 and enlargement in Figure 2-14). When both blocks are jumpered, the ISDN S/T interface is terminated at 100 ohms; otherwise, it is unterminated. The presence of the jumpers (default setting) indicates that the *DYNASTAR 100i* is the only device on the ISDN S/T interface. If the block is not jumpered, the *DYNASTAR 100i* can share the line with up to seven devices, including voice and facsimile equipment. One of the devices on the shared line must be terminated.

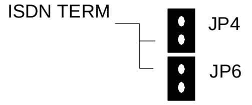


Figure 2-14 100 Ohm ISDN Termination Jumper Blocks

ADDITIONAL GROUNDING JUMPERS. Two additional grounding jumpers are located on the *DYNASTAR 100* and *DYNASTAR 100i* baseboards. These jumpers are located behind port 0 on both boards and are labeled JP14 and JP15 on the *DYNASTAR 100* and JP1 and JP2 on the *DYNASTAR 100i*. The use of these jumpers is summarized in Table 2-6.

Table 2-6 JP1/JP14 and JP2/JP15 Jumpering

Jumper Block	Configuration
JP1/JP14	1-2: signal/chassis common ground for power 2-3: isolated ground for power
JP2/JP15	1-2: signal ground for port 0 (ENET AUI) 2-3: chassis ground for port 0 (ENET AUI)

On the *DYNASTAR 100e*, jumper JP2 can be configured for signal or chassis ground, as marked on the baseboard.

PORT BIAS JUMPERS. On the *DYNASTAR 100e* and *DYNASTAR 2000*, jumpers JP3 (DTR) and JP4 (DCD) are the port bias jumpers. Jumpering pins 1-2 makes the corresponding signal *active*. Jumpering pins 2-3 makes the corresponding signal *inactive*.

DYNASTAR 500 BASEBOARD

CLEAR CONFIG JUMPER. A 2-pin jumper labeled CLR CONFIG is located on the *DYNASTAR 500* baseboard as shown in Figure 2-15. The pin pair can be used to force all configuration parameters to revert to default values. This is the only configurable jumper on the *DYNASTAR 500* baseboard.

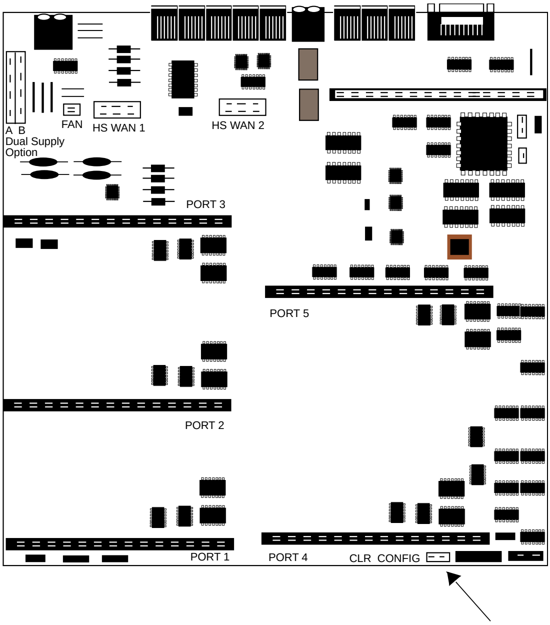


Figure 2-15 ***DYNASTAR 500* Baseboard**

To clear configuration parameter values:

1. Power off the *DYNASTAR 500*.
2. Open the front panel and locate the CLR CONFIG jumper (JP5).
3. Remove the CLR CONFIG shunt.
4. Power up the *DYNASTAR* with the shunt removed.
5. After the unit has booted, install the shunt again, leaving the *DYNASTAR* on.

✓ All settings revert to the factory defaults.

NOTE: Only the CLR/CONFIG shunt should be removed. The other shunts in the jumper block are used during board manufacture and should not be changed.

DYNASTAR 5000 BASEBOARD

CLEAR CONFIG JUMPER. A 2-pin jumper labeled CLR CONFIG is located on the *DYNASTAR 5000* baseboard as shown in Figure 2-15. The pin pair can be used to force all configuration parameters to revert to default values. This is the only configurable jumper on the *DYNASTAR 5000* baseboard.

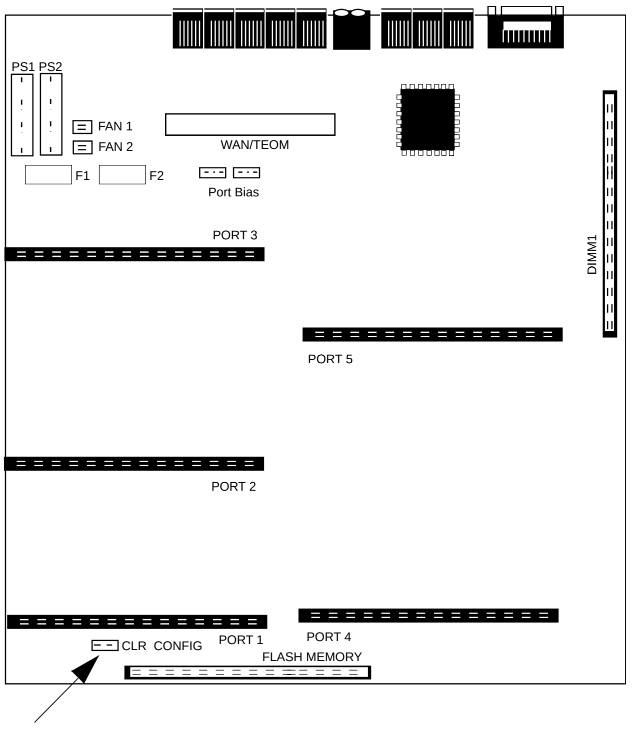


Figure 2-16 ***DYNASTAR 5000* Baseboard**

To clear configuration parameter values:

1. Power off the *DYNASTAR 5000*.
2. Open the front panel and locate the CLR CONFIG jumper (JP5).
3. Remove the CLR CONFIG shunt.

4. Power up the *DYNASTAR* with the shunt removed.
5. After the unit has booted, install the shunt again, leaving the *DYNASTAR* on.

✓ All parameters revert to the factory defaults.

NOTE: Only the CLR/CONFIG shunt should be removed. The other shunts in the jumper block are set during board manufacture and should not be changed.

JUMPER SETTINGS FOR EXPANSION MODULES

Most expansion modules consist of two parts: the expansion board, which is installed directly on the *DYNASTAR*'s baseboard, and the port connectors (also called single expansion modules), which are inserted into the rear panel of the *DYNASTAR*. This section explains the user configurable jumpers on both the expansion boards and the port connectors.

NOTE: Expansion boards and single expansion modules not mentioned in this section do not have any configurable jumpers.

NOTE: After an I/O module has been added or changed, initialize that port from the Status menu.

OCTAL+ CARD. On the OCTAL+ board, jumper block P2, shown in Figure 2-17, should not normally be jumpered for the *DYNASTAR 100* or *DYNASTAR 500*. For the *DYNASTAR 100i*, P2 should be jumpered to force DTR on.

NOTE: The OCTAL+ board is not used with the *DYNASTAR 100e*, *DYNASTAR 2000*, or *DYNASTAR 5000*.

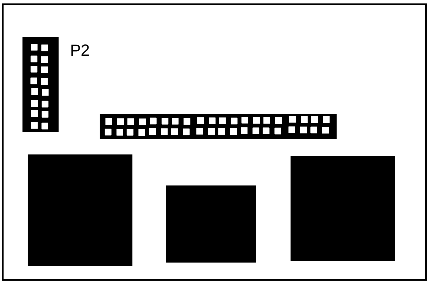


Figure 2-17 OCTAL+ Board Jumper Position

ETHERNET CARD. On the Ethernet board, you can jumper P2 for either an RJ-45 (indicated as *TP* on the board) or an AUI (DB-15) connection. If you jumper the board for an RJ-45 connection, the board is directly connected to the AUX port, and no interconnect cable is required.

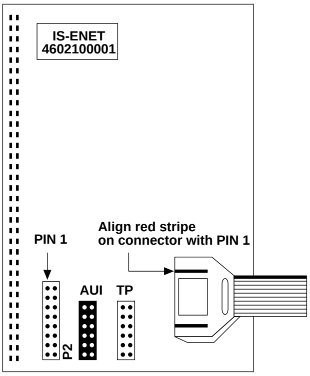


Figure 2-18 Ethernet Board Jumper Positions

If you have set the jumper for an AUI connection, you must install Cable 4602230001. Attach the 16-pin female connector on the end of the cable to P2 on the Ethernet daughterboard. Align the red stripe on the cable with Pin 1 on the board as shown in Figure 2-18. Connect the other end of the cable to the Ethernet slot (Port 0 ENET AUI) on the backplane of the *DYNASTAR*.

NOTE: The Ethernet board is not used with the *DYNASTAR 100e, DYNASTAR 2000,* or *DYNASTAR 5000.*

SINGLE EXPANSION MODULES. Several of the expansion boards can be configured with single expansion modules that provide a variety of interfaces. (See Chapter 1, *Introduction*, for a complete list of single expansion modules.) Those that have configurable jumpers are discussed below.

The **X.21**, **V.24/RS-232**, and **V.35** single expansion modules (Figure 2-19) provide a DB-15 female connector and can be used in any combination on the QUAD card.

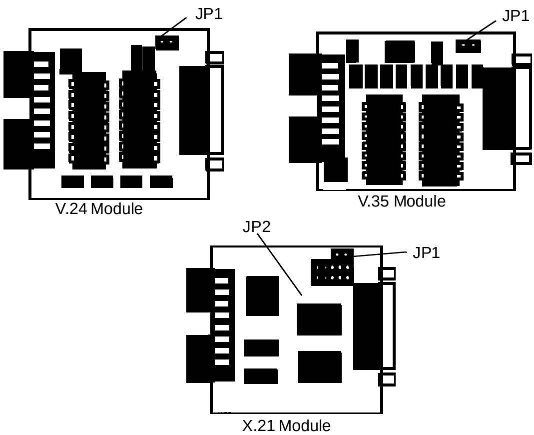
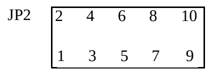


Figure 2-19 V.24/RS-232, V.35, and X.21 Single Expansion Modules

Each of these single expansion modules contains jumper block JP1. This jumper block determines whether chassis ground (Pin 1) is used. To enable chassis ground, insert the jumper onto jumper block JP1. To disable chassis ground, remove the jumper from jumper block JP1.

The X.21 module contains a second jumper block, JP2, which can be used to configure DCE or DTE resistor termination. The board is delivered with all jumpers installed. In this factory configuration, DTE or DCE operation can be selected from software, and it is not necessary to change any jumpers on the board. However, although the board provides full X.21 functionality when configured this way, it is not technically fully compliant with the X.21 recommendation for impedance.

If you require full X.21 technical compliance, you will need to configure jumper block JP2 for DTE or DCE operation as illustrated in Figure 2-20, in addition to making the software selection for DTE or DCE.



PINS	DCE	DTE
1 - 2	IN	OUT
3 - 4	IN	OUT
5 - 6	OUT	IN
7 - 8	OUT	IN
9 - 10	OUT	IN

IN = jumpered

OUT = not jumpered

Figure 2-20 DCE/DTE Configuration for JP2 on Quad Port Connectors

The **RS-485** single expansion board (Figure 2-21), which is supported on the baseWAN ports (4/5 or 8/9) and on the QUAD or 8-port expansion modules, provides a DB-15 female connector and has two configurable jumper blocks, J2 and J3.

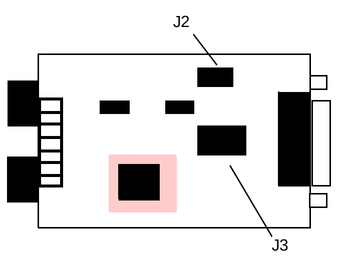


Figure 2-21 RS-485 Single Expansion Module

Jumper block J2 (Figure 2-22) is a 3-pin jumper that provides 120-ohm termination or non-termination of the balanced pair. To provide non-termination, place the jumper over the two pins marked *open*. To provide termination, place the jumper over the two pins marked *term*. Non-termination is the default setting.

Jumper block J3 (Figure 2-22) provides 2 rows of 4 pins each. This jumper block provides biasing, or not, on the receive or transmit pairs. To provide biasing on the receive pair, place the jumper in each row over the two pins marked *rcv*. To provide biasing on the transmit pair, place the jumper in each row over the two pins marked *xmt*. To provide no biasing, place the jumper in each row over the two pins marked *none*. The default is no biasing.

Figure 2-22 Jumper Blocks J2 and J3 on the RS-485 Single Expansion Module

■ ADDING AN EXPANSION BOARD

DYNASTAR 500 AND *DYNASTAR 5000*

You can change the physical configuration of your *DYNASTAR 500* or *DYNASTAR 5000* by installing different expansion boards in any of the five expansion slots on the baseboard. These expansion slots are numbered as shown in Figure 2-15. Each slot, when properly cabled to the matching internal connector on the backplane (Figure 2-23), corresponds to a specific row of connectors on the back panel and to the matching LEDs on the front panel. After you install the expansion board, you must also install the corresponding port connectors in the rear panel. The cabling and connectors used for each type of expansion board are summarized in Table 2-7.

For an overview of the functionality of each expansion module, see Chapter 1, *Introduction*.

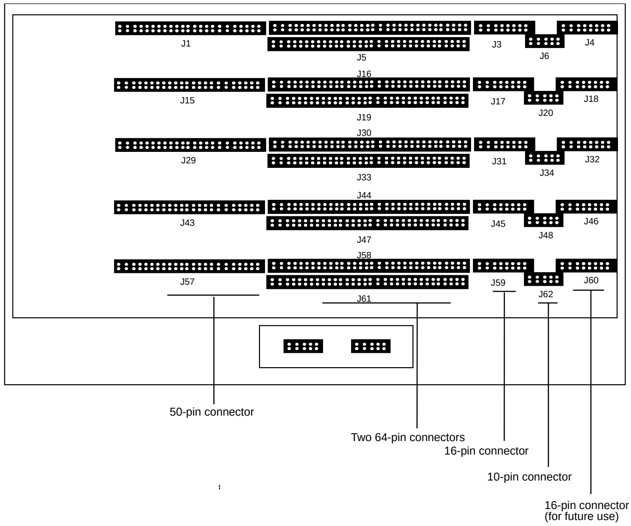


Figure 2-23 Internal Backplane Connectors for *DYNASTAR 500* and *DYNASTAR 5000* Expansion Modules

Table 2-7 Expansion Module Connectors and Cables

Expansion Module	Connectors
QUAD	64-pin ribbon into lower connection of pair, that is, J5, J19, J33, J47, J61
OCTAL+ (*DYNASTAR 500* only)	50-pin ribbon
ENET	16-pin ribbon
8-Port Sync/Async 16-Port Sync/Async Contact Ethernet Hub	2 x 64-pin ribbon into both J2/J5, J16/J19, J30/J33, J44/J47, J58/J61

Table 2-7 Expansion Module Connectors and Cables (cont.)

Expansion Module	Connectors
T1/E1 PRI T1/E1 Channelized BRI	2 x 16-pin ribbon Trunk 1: P3 on board to J4, J18, J32, J46, or J60 Trunk 2: P4 on board to J3, J17, J31, J45, or J59

NOTE: The CSU/DSU module is not installed in the standard expansion slots. If you have ordered this capability, it will be pre-installed for you at the factory.

To install an expansion module in the *DynaStar 500* or *DynaStar 5000*:

1. Power off the *DynaStar*.
2. Connect the appropriate cable to the back of the expansion board.
3. Loosen the screw and open the front panel of the *DynaStar*.
4. Locate the correct slot on the baseboard and align the pins on the underside of the expansion board with the slot (Figure 2-15). Align the pins so that the left sides (as viewed from the front of the unit) are flush. (Some modules do not require all the pins on the baseboard header.)
5. The expansion board has two holes for mounting on the half-inch support posts. Make sure that the expansion board is connected to the support posts (Figure 2-24). Press down until the pins on the underside are no longer visible.

✓ The expansion board should snap firmly into place.

Figure 2-25 shows a *DynaStar 500* baseboard with an expansion board installed.

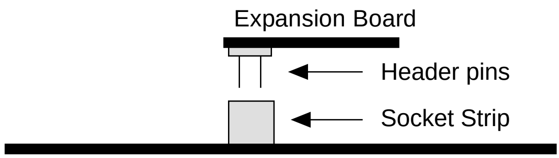


Figure 2-24 Side View of Baseboard with Expansion Board

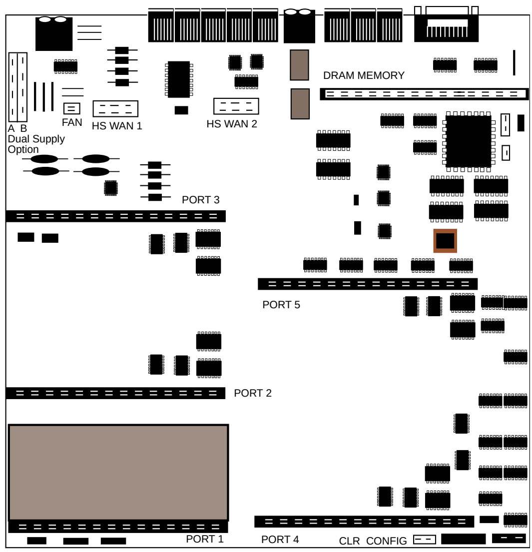


Figure 2-25 *DYNASTAR 500* Baseboard with Expansion Board

6. Connect the loose end of the expansion board cable to the matching connector in the row that corresponds to the expansion board slot. Be sure that the red stripe on the cable is to the right.

   NOTE: For the 16-port expansion boards, there are two 64-pin cable ends that must be connected to the two 64-pin connectors in the row.

7. Close the front panel.

8. Turn the *DYNASTAR* around so that the rear panel is facing you. Insert the corresponding port connectors in the correct row and fasten them with the screws provided.

DYNASTAR 100/100i/100e/2000

You can also add an expansion module to your *DYNASTAR 100* or *DYNASTAR 100i*. However, there is only one expansion slot on the *DYNASTAR 100/100i* baseboard, so only one expansion board can be added. Figure 2-6 illustrates the location of the expansion slot on the *DYNASTAR 100* baseboard.

The *DYNASTAR 100e* and the *DYNASTAR 2000* accept two expansion boards, as shown in Figure 2-8. The procedure for installing expansion boards is the same for the *DYNASTAR 100* models and the *DYNASTAR 2000*.

For an overview of the functionality of each expansion board, see Chapter 1, *Introduction*.

NOTE: If you have ordered the CSU/DSU module, it will be pre-installed for you at the factory.

To install an expansion module:

1. Connect the appropriate cable to the expansion board.
2. Loosen the screws on the back panel of the *DYNASTAR* and slide the baseboard from the unit.
3. Align the pins on the underside of the expansion board with the pins in the slot on the baseboard so that the first pin on the expansion module aligns with the slot marked *1* on the baseboard. (Some modules are smaller and do not require all pins on the baseboard header.)
4. An expansion board has two mounting holes on the half-inch support posts. Make sure that the expansion board is connected to the support posts. Press down so the pins on the underside are not visible (Figure 2-24).

✓ The expansion board should snap firmly into place.

5. Connect the ribbon cable on the expansion board that you installed in your unit to the corresponding port connectors.

   NOTE: Depending on which expansion board you installed, you may have to connect several ribbon cables. For example, the Quad card

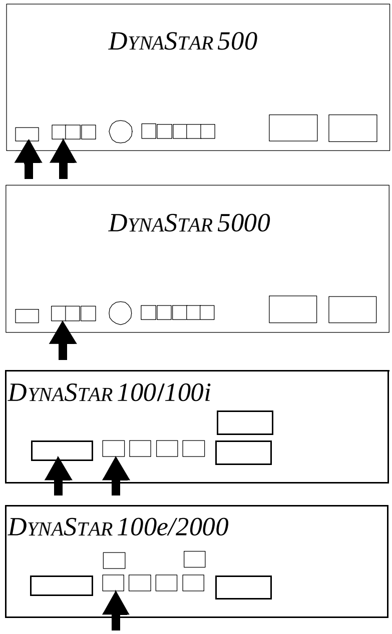
uses a 64-pin ribbon cable that has been split four ways to connect to each of the four port connectors.

6. Insert the ports through the corresponding opening in the rear panel of the *DYNASTAR* and fasten them with the screws provided.
7. Reinsert the baseboard into the chassis and tighten the screws that hold it into place.

PORT CONFIGURATION OVERVIEW

The procedure for setting up your *DYNASTAR* to support your required connections consists of three main steps. You must first configure the hardware as required. This was discussed in the earlier sections of this chapter. You then have to make the required physical connections. This is explained in the section that follows (*Physical Connections*). The last step is to configure the required connection(s) in software. This step is summarized in the section *Software Configuration* later in this chapter.

CONNECTING A LAN



Either the Ethernet AUI or 10BASE-T connector on the rear panel can be used for a LAN connection. To support a second connection, an expansion board must be added. This provides access either to a 10BASE-T connection through the AUX port or an additional hardware connection above the main row of connectors.

NOTE: The *DYNASTAR 100e*, *DYNASTAR 5000,* and *DYNASTAR 2000* support 10/100BASE-T.

To connect to the LAN:

1. Plug one end of the Ethernet cable into the LAN port.

   To connect to a 10BASE-T Ethernet, use a twisted-pair modular cable terminated with an 8-pin modular (RJ-45) plug. Plug the RJ-45 modular plug into the 10BASE-T connector on the rear panel of the *DYNASTAR*.

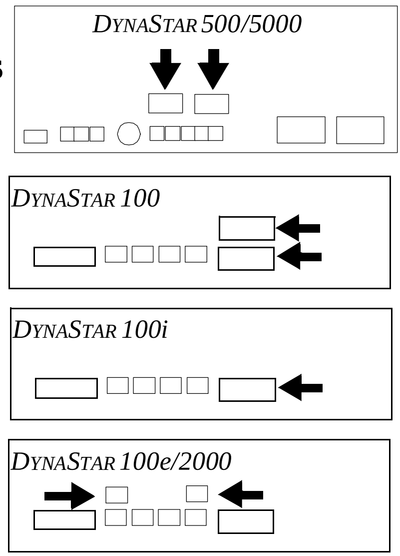
If you are connecting a thick Ethernet cable, attach a transceiver between the AUI connector and the Ethernet cable.

2. Plug the other end of the cable into an Ethernet hub or concentrator.

3. Once both ends of the cable are connected, verify that the Link Detect LED on the hub is lit.

✓ Within 30 seconds, the Ethernet LED on the *DynaStar* will turn green if the LAN is active and operational.

HS WAN Connections



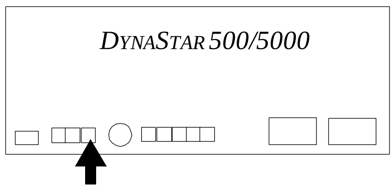
For router, Ethernet bridge, frame relay, synchronous PPP, and X.25 applications, use the HS WAN V.35, X.21, or V.24/RS-232 ports (ports 8 or 9 on the *DynaStar 500* and *DynaStar 5000*; ports 4 or 5 on the *DynaStar 100/100e/ 2000*; port 5 only on the *DynaStar 100i*) to support a synchronous connection to another router or bridge or to an X.25 or frame relay network.You can also use expansion card ports that support synchronous protocols.

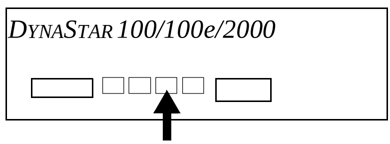
The T1/E1, DDS, and Modem single expansion modules are also available for the base WAN ports (ports 4 and 5) on the *DynaStar 100e* and the *DynaStar 2000* only

Use one of the HS WAN ports to connect a synchronous data service unit (DSU) for V.35, X.21, or V.24/RS-232 interfaces. To connect a synchronous line to one of the ports:

1. Plug the male DB-15 connector on one end of the cable into one of the HSWAN ports (V.35, X.21, V.24/RS-232).
2. Plug the connector on the other end of the cable into your modem or DSU.

RS-232/V.24 CONNECTIONS





The synchronous/asynchronous port (port 7 on the *DYNASTAR 500/5000*; port 3 on the *DYNASTAR 100*/*100e/2000*) can be configured to support synchronous or asynchronous operations for the RS-232/V.24 signaling interface. The default configuration is for synchronous operation with a PPP interface.

NOTE: On the *DYNASTAR 100i*, the two B channels replace one of the HS WAN ports and the synchronous/asynchronous port of the *DYNASTAR 100*.

Or you can connect to any port on an expansion board that supports RS-232/V.24 connections.

The RS-232/V.24 connector is an RJ-69 modular interface. To connect a synchronous or asynchronous line to the RS-232/V.24 port:

1. Plug the RJ-69 modular connector into the port.

NOTE: This is an RJ-45/RJ-69 connector that uses 8 wires for asynchronous transmission and 10 wires for synchronous transmission.

2. Plug the other end of the cable into a synchronous/ asynchronous adapter that plugs into the modem or DSU. (You can also connect locally.)

DEBUG PORT

The Debug Port is located at the far left of the bottom row of connectors on the back panel of the *DYNASTAR* 2000 (Figure 1-6) and the *DYNASTAR 5000* (Figure 1-7). It is a standard RS-232/V.24 interface that operates as a DCE at 9600 bps (7 bits, even parity, 1 stop bit).

SOFTWARE CONFIGURATION

Detailed information on using the screens to configure your ports and connections are given in the chapters that follow. The steps below provide a configuration guideline.

1. Configure the protocol that will be used on the port (SNA, frame relay, synchronous PPP, transparent, or X.25 for synchronous lines; PAD, async PPP, IPX-In, IPX-Out, IPX-In/Out, or SLIP for asynchronous lines).
2. For router applications, verify the IP/IPX/OSI addresses and configure static routes if required (Router menu).
3. For X.25 applications, configure any required X.121 switching table entries.
4. For async services (PAD, Telnet, IPX-In, SLIP, X25/In, X25/Out), configure additional information in the Async Services menu.
5. Configure any required security (PAP/CHAP, etc.).

■ SPECIFICATIONS

Table 2-8 *DYNASTAR* Specifications

	Height	**Width**	**Depth**
DYNASTAR 100	1.75" (4.45 cm)	17.25" (43.8 cm)	9.5" (24.23 cm)
DYNASTAR 2000	3.25" (8.25 cm)	17.25" (43.82 cm)	9.5" (24.23 cm)
DYNASTAR 500	8.25" (20.98 cm)	17.25" (43.82 cm)	13" (33.02 cm)
DYNASTAR 5000	8.25" (20.98 cm)	17.25" (43.82 cm)	13" (33.02 cm)

NOTE: The *DYNASTAR 100* columns in Table 2-8 refer to the *DYNASTAR 100*, *DYNASTAR 100i*, and *DYNASTAR 100e*. The *DYNASTAR 2000* columns refer to both the *DYNASTAR 2000* and *DYNASTAR 2000H*.

THE SUPERVISOR

■ INTRODUCTION

The *DYNASTAR* Supervisor is used to perform the following tasks:

- Configure each port's interface protocol and parameters
- Enable and disable individual ports
- Monitor the status of the *DYNASTAR*
- Monitor the status of individual ports and calls
- Monitor protocol statistics
- Restrict operator access
- Add new applications
- Initiate a download from/to another *DYNASTAR*
- Warm or cold start the *DYNASTAR*
- Establish dialup connections

This chapter tells you how to connect to the Supervisor Console, log in, move through the menus, change passwords, and set access permissions.

■ Supervisor Console Connection Options

After the *DynaStar* is installed and tested, a workstation or a remote terminal can be used as the Supervisor Console. Port 6 can then be reconfigured for other applications.

NOTE: The console must be set for 7 bits, even parity, and 1 stop bit.

The Supervisor Console can also be connected to the Supervisor via a dialup connection or via a network, or you can connect to the Supervisor from a LAN workstation.

A system administrator can manage multiple *DynaStars* from one Supervisor Console. When the *DynaStar* is configured with a dialup console port or a network line, the administrator can log in to the Supervisor from anywhere on the WAN.

Dialup Connection

To connect the Supervisor Console to the Supervisor via a dedicated or dialup connection:

1. Connect a null modem between the modem and the *DynaStar*. (This is necessary when you first receive the *DynaStar* from the factory because the Supervisor Console port is configured as a DCE at the physical level by factory default.)
2. Turn the Supervisor Console on.
3. Make a dialup connection to the console port of the *DynaStar*.
4. Press **<return>** twice to transmit the Supervisor Console's speed (9600) and parity (even).

✓ You are automatically connected to the Supervisor. The Login menu appears.

X.25 Network Connection

To connect the Supervisor Console to the Supervisor through an X.25 network:

1. From an attached terminal, connect to a network's PAD and proceed as required by its terminal's interface.
2. To make a call to the *DynaStar* Supervisor port, enter the X.121 address of any physical port followed by 99 and press **<return>**.

✓ When the connection has been made, an X.28 connected message is displayed, and the Login menu appears.

If the connection fails, one of these messages appears:

- *CLR OCC* (or equivalent) means another Supervisor call is active.
- *CLR IDLE* (or equivalent) means there has been no activity on your call for three minutes, and the call has been automatically cleared.
- *CLR NP* (or equivalent) means that a valid path does not exist through the X.25 network.Verify that the correct X.121 address was used to place the call.

Connecting from a LAN Workstation

For IP, simply call the *DynaStar*'s IP address from a Telnet client on port 23.

NOTE: If the data call to the Supervisor clears, type **9999** to place another call, or retry at the PAD prompt.

■ Login Procedures

When your system starts up, the Login menu displays the supervisory herald and the software version number, as shown in Figure 3-1. You receive a prompt for the Supervisor’s password.

If you log in from a LAN, the Telnet connection screen, shown in Figure 3-2, appears before the Login menu. Select **1** on the Telnet connection screen to go to the console and access the login screen.

NOTE: If you are using SecurID, see *SecurID Login Instructions* later in this chapter.

To log in:

1. At the **Enter Password** prompt, type your password and press **<return>**. The password ***is*** case sensitive.

   NOTE: The first time you log in, type **secret** and press **<return>**.

✓ A screen similar to the one in Figure 3-3 appears, asking you to identify your console type.If you do not enter a valid password in three attempts, the data call to the Supervisor is cleared, and you receive the X.28 PAD message *CLR PAD*. To be reconnected to the Supervisor, enter **9999** and press **<return>** or shut the console off and then turn it on again.

```
DynaStar Supervisor

DynaStar 500
Software Version number - 6.07.3

Copyright (c) 1990-2002

Press ESC to exit Supervisor
To get back into Supervisor, type 9999 <RET>

Enter Password:
```

Figure 3-1 Login Menu for the *DYNASTAR 500*

```
Telnet> 100.1.1.1
Trying to establish connection....
Connected



DynaStar_6aea services


   1   CONSOLE   6aea
   2   X25PDN     PAD665

Enter service selection: Telnet>
```

Figure 3-2 Initial Login Screen when Connecting from a LAN

```
DynaStar Supervisor

DynaStar 500
Software Version number - 6.07.3

Copyright (c) 1990-2002

Press ESC to exit Supervisor
To get back into Supervisor, type 9999<RET>

Enter Password:

Supervisor Console Type
      1 - Wyse 50 or TVI-910/920
      2 - VT100 or ANSI compatible

Enter Console Type:
```

Figure 3-3 Login Screen with Console Type Selection

2. Enter your console type as either **1** (Wyse 50 or TVI-910/920) or **2** (VT100 or ANSI compatible), and press **<return>**.

✓ The Main menu appears, as shown in Figure 3-4.

NOTE: The first time you connect to the Supervisor, you should immediately change the default password. Be sure to change passwords periodically.

```
                        ***Main Menu***

1 - Status              Board, addresses, stats, enable/disable, error log
2 - Call status/control Call set-up, disconnect, status
3 - Configuration       Dial directory, port, and application parameters
4- System functions     Date/time, applications, software load, restart
5 - Security            Supervisor passwords, IPX-in/out security



                     Enter command number:



_______[DynaStar dc000345]_______
Terminate input with <RET>.              Press ESC to return to previous menu.
```

Figure 3-4 Main Menu

■ UNIVERSAL COMMANDS FOR NAVIGATING WITHIN THE SUPERVISOR

The five sets of *DYNASTAR* menus are summarized on the Main menu as shown in Figure 3-4. Each set of menus is a separate hierarchy.

To move down through a set of menus:

1. In the **Enter command number** field, type the number that appears next to the menu you want to display.
2. Press **<return>**.

To return to the previous menu in the hierarchy:

1. Press **<ESC>**.
   If you use **<ESC>** to escape from the Login menu, your call to the Supervisor is cleared.

To enter new information in menus:

1. Use the cursor keys (left, right, up, down) to move around the fields.

   NOTE: If the cursor keys do not work correctly (they cause a jump to the previous menu), the cursor keys are not set correctly in the terminal application. For Windows and VT100, select VT100 arrows, not Windows arrows, to correct the problem.

2. Depending on the field, enter new information by typing in the new value or by pressing **<return>** to toggle through the available values. The two ways of entering information are mutually exclusive. In fields where you toggle to enter the values, go to the next field by pressing **<tab>**.

3. Move the cursor to the **Process selections** field.

4. Enter **Y** and press **<return>** (or simply press **<return>**) to instruct the Supervisor to process the new information.

   OR

   Enter **N** and press **<return>** to abort your input and return to the previous menu. This is equivalent to pressing **<ESC>** at any position on the menu.

   NOTE: You can usually move the cursor directly to the **Process Selections** field by positioning it in the leftmost field on a line and pressing the left arrow.

   NOTE: Commands available on a menu are summarized at the bottom of the menu.

Editing Input

The Supervisor Console is preconfigured to use the following editing characters:

WYSE Character	ANSI/VT100 Character	Function
DEL	BS	Deletes the last character
CTRL-X	DEL	Deletes a field of input

Command Notation

Throughout this manual, the following notation is used:

- The names of keys are bold and contained in angle brackets: **<return>**.
- When two keys are pressed simultaneously, they appear in angle brackets separated by a hyphen: **<CTRL-D>**.
- Commands you must enter appear in **boldface**.
- The names of menu fields also appear in **boldface**.
- Representative text in a command line appears in *italics*. For example, the word *filename* indicates that the actual name of a file is to be entered.
- System messages appear in *italics*.

■ SAVING CHANGES TO FLASH MEMORY

As you configure the *DYNASTAR*, you will be reminded to save your changes to Flash Memory by this highlighted message: *Config has changed: use CTRL-W to save.* If you press <**CTRL-W**>, the message *Saving configuration to Flash...* appears. Once the save is complete, the message disappears and the *DYNASTAR* beeps to alert you.

NOTE: Be sure to save changes using the CTRL-W command before restarting the *DYNASTAR*.

■ THE SUPERVISOR'S MENU HIERARCHY

The Main menu of the *DYNASTAR* Supervisor, shown in Figure 3-5, provides access to these items: Status, Call Control, Configuration, System functions, and Security.

```
                              ***Main Menu***

1 - Status                Board, addresses, stats, enable/disable, error log
2 - Call status/control   Call set-up, disconnect, status
3 - Configuration         Dial directory, port, and application parameters
4 - System functions      Date/time, applications, software load, restart
5 - Security              Supervisor passwords, IPX-in/out security


                           Enter command number:


_______[DynaStar dc000345]_______
Terminate input with <RET>.                 Press ESC to return to previous menu.
```

Figure 3-5 ***DYNASTAR* Main Menu**

Selecting one of these items presents a menu hierarchy. The Main menu hierarchy is illustrated in Figure 3-6.

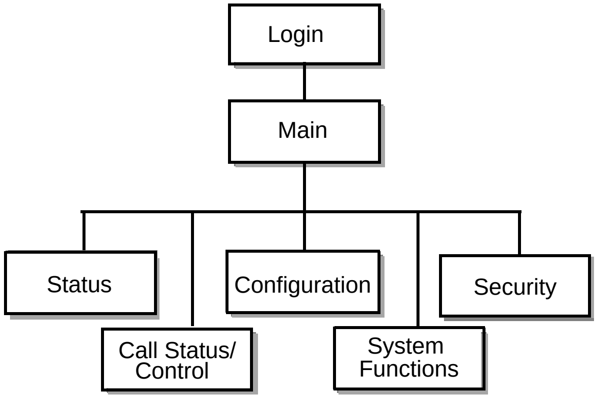
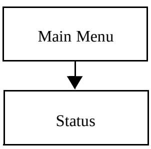


Figure 3-6 Main Menu Hierarchy

Hierarchies for the Status, Call Status/Control, Configuration, System Functions, and Security menus are shown in the pages that follow.



STATUS MENUS

```
*** Status Commands ***

1 -   Board Status          Display internal module types and status
2 -   Call status           Check call status and manually disconnect calls
3 -   Names/Addresses       Verify names & MAC, IP, IPX and X.121 addresses
4 -   Statistics            Show statistics for port n
5 -   Buffer Usage          System buffer usage
6 -   Disable Port          Put port n in Disabled state (busy out dial ports)
7 -   Enable Port           Bring port n to an Enabled state
8 -   Initialize Port       Perform initialization on port n
9 -   Log                   Display system error log
10 - Monitoring             Show input/output data packets for port n
11 - Busy/UnBusy Port       Bring port n to Busy/UnBusy state
12 - PPP status             Check call status
13 - OSI                    OSI operator console
14 - Modem Status           Show statistics & status for modem resources
15 - Call History           Show status of transactions per ISDN port
16 - Trace                  SNA Trace

                            Enter command number:

_________[DynaStar_3df2]__________
Terminate input with <RET>.              Press ESC to return to previous menu.
```

Figure 3-7　Status Commands Menu

Status menus are used to check or change the status of the *DYNASTAR*. The Status Commands menu (Figure 3-7) consists of 16 selectable commands, mapped out in Figure 3-8.

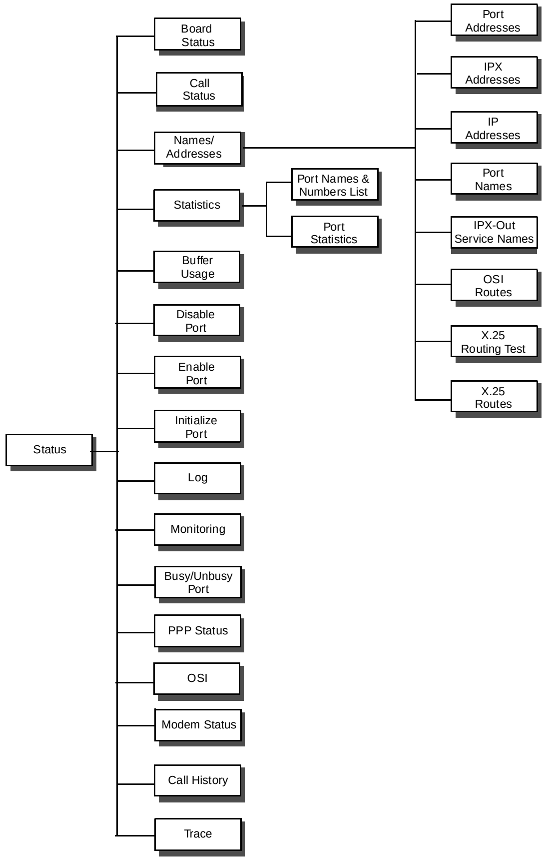
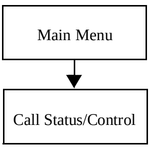


Figure 3-8 Status Menu Hierarchy



Call Status/Control Menu

```
                    *** Call Status/Control Commands ***

1 -  Manual call setup          Select locations to call
2 -  Call status/disconnect     Check call status and manually disconnect calls
3 -  X.25 connections           Check X.25 Call status
4 -  User call status           Check connected users
5 -  TCP connections            Check TCP connection status
6 -  VPN connections            Check VPN connection status
7 -  Frame Relay DLCIs          Check Frame Relay DLCI connection status



                          Enter command number:


_________[DynaStar_3df2]__________
Terminate input with <RET>.              Press ESC to return to previous menu.
```

Figure 3-9 Call Status/Control Commands Menu

The Call Status/Control menu provides access to screens used to set up automatic and manual dial-up connections and to monitor these connections. The hierarchy for the Call Status/Control Menu is shown in Figure 3-10.

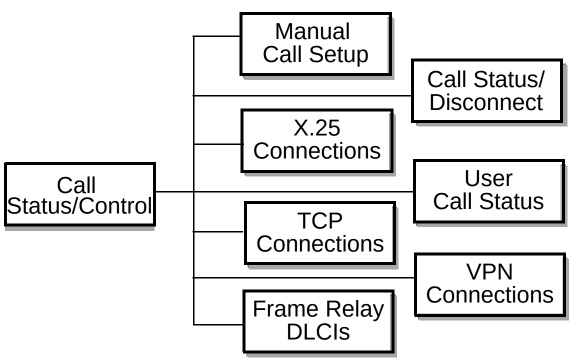
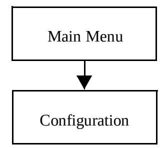


Figure 3-10 Call Status/Control Menu

CONFIGURATION MENU




```
                    ***Configuration Commands***

1 -  PPP dial directory      Locations, telephone numbers, option selection
2 -  Port                    Protocol, connection mode, line speed, addresses
3 -  Router                  IPX & IP addresses, static routes, IP filters
4 -  Bridge                  STP & dial parameters, Bridge filters
5 -  Frame Relay             DLCIs for SNA, routing/bridging, and FR-ATM
6 -  Async services          PAD, Telnet, IPX-In, SLIP parameters
7 -  Server                  System-wide parameters (Heralds, idle timers)
8 -  SNMP                    Community strings, trap addresses, authentication
9 -  PAP/CHAP table          Allowed PAP/CHAP authentication values
10 - X.25                    X.121 addresses, switching table
11 - ATM                     VPI/VCIs for MPOA and FR Interworking
12 - SNA                     Change/verify SNA parameters
13 - OSI                     Change/verify OSI parameters
14 - Modem Classes           Change/verify Modem parameters
15 - Contact Board/TBOS      Add/Change/Verify the alarm parameters

                      Enter command number:

_______[DynaStar dc000345]_______
Terminate input with <RET>.              Press ESC to return to previous menu.
```

Figure 3-11 Configuration Commands Menu

Configuration menus are used to verify and change configuration parameters. The Configuration menu (Figure 3-11) consists of the selectable commands shown in Figure 3-12.

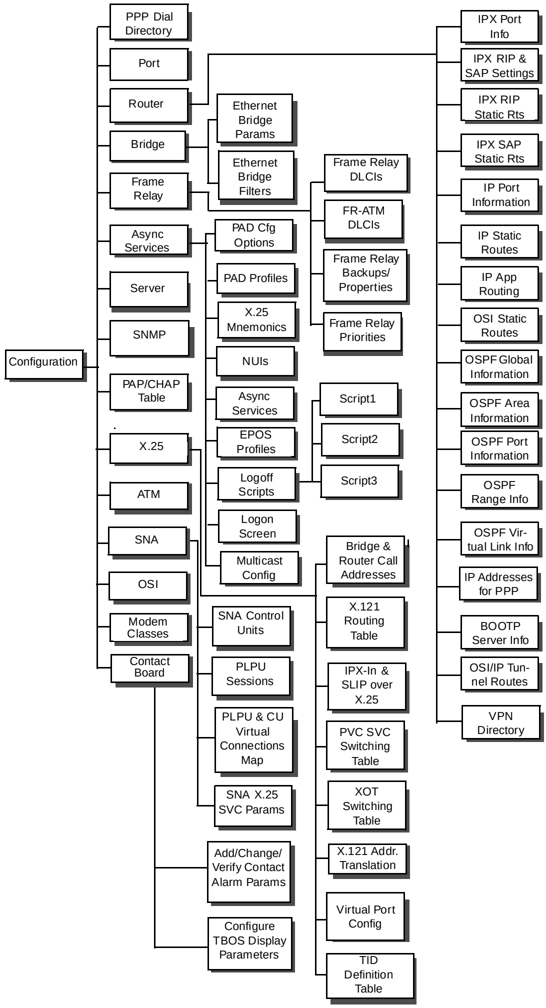
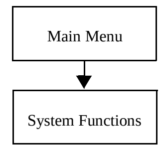


Figure 3-12 Configuration Menu Hierarchy



THE SYSTEM FUNCTIONS MENU

```
                    ***System Commands***

1 -  Date & Time         Set the system date and/or time
2 -  Applications        Activate applications and check versions
3 -  Load code           Update system software
4 -  Warm restart        Restart system
5 -  Cold restart        Restart system & reset config to default values
6 -  Reinitialize        Restart system & reset config from cnfgload.cmp
7 -  Code versions       Display downloaded software versions



                    Enter command number:


_______[DynaStar dc000345]_______
Terminate input with <RET>.              Press ESC to return to previous menu.
```

Figure 3-13   System Functions Menu

The System Functions menu (Figure 3-13) provides access to menus for setting system time, activating applications, loading code, and restarting the *DYNASTAR*. The menu hierarchy for the System Functions menu is shown in Figure 3-14.

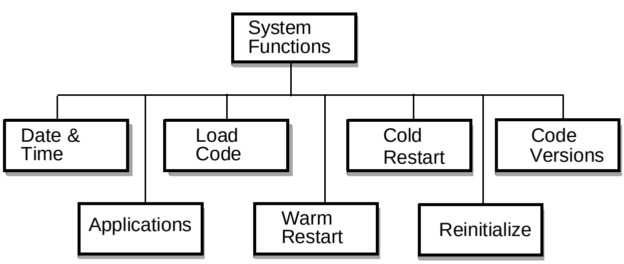
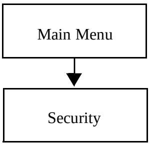


Figure 3-14   System Functions Menu Hierarchy



SECURITY COMMANDS MENU

```
                    ***Security Commands***

1 -  Password Change      Change Operator Password
2 -  Access Security      Change Operator Access
3 -  IPX-In Security      IPX-In ID strings
4 -  IPX-Out security     IPX-Out service restrictions
5 -  IP Filter            IP Address Filter
6 -  TL1 security         Add/Change TL1 Username/Password
7 -  Network security     Add/Change Network Passwords
8 -  Destinations         Add/Change Permitted Destinations
9 -  Security Options     Validation options and methods
10 - SecurID              Access Authorization
11 - Port Selection       Which ports have security enforced


                    Enter command number:


_______[DynaStar dc000345]_______
Terminate input with <RET>.            Press ESC to return to previous menu.
```

Figure 3-15 Security Commands Menu

The Security Commands menu (Figure 3-15) provides security and allows the user to set several types of access restrictions for the *DYNASTAR*. The Security Commands menu hierarchy is shown in Figure 3-16.

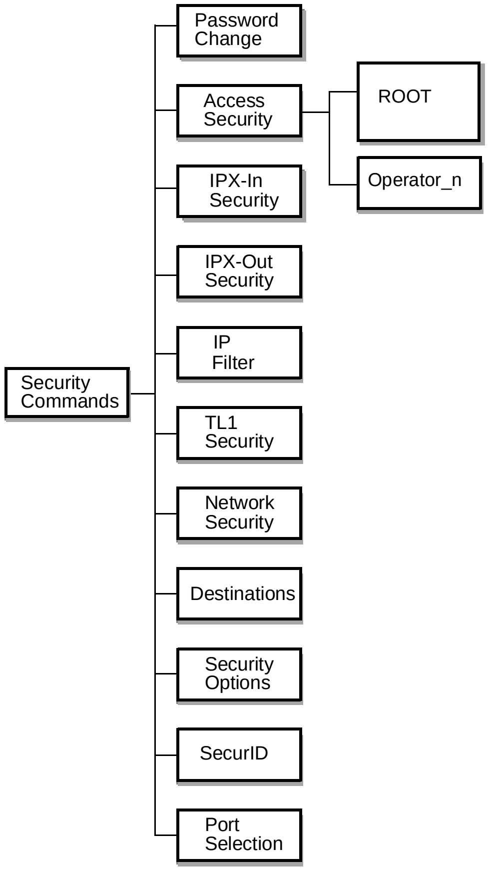


Figure 3-16 Security Commands Menu Hierarchy

■ Operator Access

Multi-Level Operator Access

In addition to the standard root access, the *DynaStar* supports up to five additional operator authorizations. The additional operators and their access authorizations are defined by the root user. By default, the five operators are named Operator_1, Operator_2, and so on, and they have no access to any functions. The root user can change the names and access capabilities of these operators.

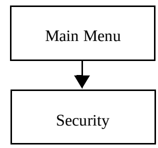
Three levels of access are available: No Access (N), Read-Only Access (R), and Write Access (W). No Access blocks the operator from accessing a given group of commands; Read-Only Access allows the operator to view parameters but not change them; and Write Access provides the ability to read and modify parameters. By default, No Access is assigned to all operators for all groups of commands. The root user always has Write Access to all commands.

The default passwords for the five operators are **Operator1**, **Operator2**, and so on. The root user should change these passwords, as well as the root user password, as soon as the *DynaStar* is installed. Each operator must have a unique password. The system will reject any duplicate password and prompt the root user for another one.

To configure the operator access:

1. From the Main menu, select **Security**.

✓ The Security Commands menu (Figure 3-17) appears.

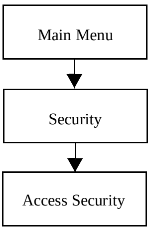



```
                         ***Security Commands***

1 -   Password Change       Change Operator Password
2 -   Access Security       Change Operator Access
3 -   IPX-In Security       IPX-In ID strings
4 -   IPX-Out security      IPX-Out service restrictions
5 -   IP Filter             IP Address Filter
6 -   TL1 security          Add/Change TL1 Username/Password
7 -   Network security      Add/Change Network Passwords
8 -   Destinations          Add/Change Permitted Destinations
9 -   Security Options      Validation options and methods
10 - SecurID                Access Authorization
11 - Port Selection         Which ports have security enforced


                         Enter command number:


_______[DynaStar dc000345]_______
Terminate input with <RET>.               Press ESC to return to previous menu.
```

Figure 3-17   Security Commands Menu

2. Select **Access Security**.

✓ The Operator Access menu shown in Figure 3-18 appears.



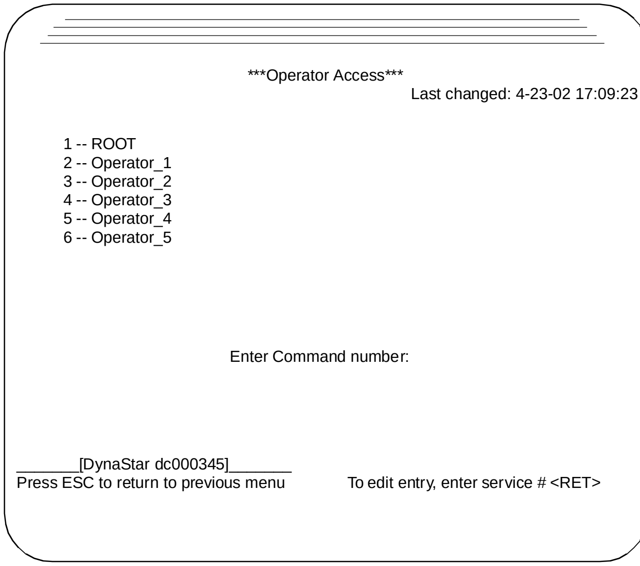
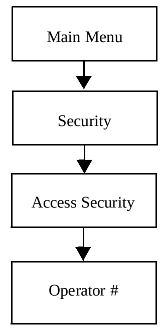


Figure 3-18 The Operator Access Menu

3. In the **Enter Command number** field, enter the number of the operator whose access authorization you want to change.

✓ The Access Control menu for the designated operator appears, as shown in Figure 3-19.




```
                    ***Operator Access Selections***
                                          Last changed: 4-23-02 18:44:56

      Menu                                  Permissions

1 -   Main Menu                                 N
2 -   Status Commands                           N
3 -   Call Control Commands                     N
4 -   Configuration Commands                    N
5 -   System Commands                           N
6 -   Security Commands                         N
7 -   Verify Names and Addresses Commands       N
8 -   Router Commands                           N
9 -   Bridge Parameters                         N
10 - Frame Relay Parameters                     N
11 - Access Server Commands                     N
12 - Async Service Names                        N
13 - X.25 Parameters                            N
14 - Async Services                             N
15 - Network Security Information               N

                                     User Name: Operator_1

_____DynaStar_834d_____________           Process selections (Y/N): Y
<RET> to toggle or type value         Use <TAB> and CURSOR to move fields
Press ESC to return to previous menu.
```

Figure 3-19 The Access Control Menu

4. Set the authorizations as required for each available category.

5. When you have finished configuring the operator access, enter **Y** in the **Process selections** field and press **<return>**.

Changing the Operator Name or Password

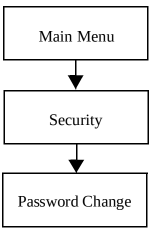
NOTE: For information on changing a SecurID password, see *SecurID* later in this chapter.

To change the password of the root user or an operator:

1. From the Main menu, select **Security**.

✓ The Security Commands menu, similar to Figure 3-17, appears.

2. Select **Password Change**.



✓ A Console User Directory screen, similar to Figure 3-20, appears.

```
                    *** Console User Directory ***
                                      Last changed: 5-5-02 08:44:53

     User Name                        Password
     <16 chars max>                   <16 chars max>
   0 -- ROOT                          Password Accepted
   1 -- Operator_1                    Password Required
   2 -- Operator_2                    Password Required
   3 -- Operator_3                    Password Required
   4 -- Operator_4                    Password Required
   5 -- Operator_5                    Password Required




_____DynaStar_834d________                  Process selections (Y/N): Y
Use <CTRL-D> to delete entry          <RET> to toggle or type value
                                      Press ESC to return to previous menu.
```

Figure 3-20 The Change Password Menu

3. To change the user name, move to the operator name you wish to change and type in the new name.

4. Tab to move to the **Password Required** (or **Password Accepted)** field and type in the new password.

NOTE: The password is case sensitive.

5. Press **Enter**.

✓ **Re-enter password** appears on the screen.

6. Re-enter the password and press **<return>**.

✓ **Password Accepted** is displayed.

NOTE: The passwords are not echoed to the screen, so be sure to remember them.

7. Enter **Y** in the **Process selections** field and press **<return>**.

WARNING: Be sure to remember the root password and protect it. If you lose or forget your password,

there is no way to gain access to the console port, and you must cold start the *DYNASTAR* to gain access. For information, see the section *Cold Starting the DYNASTAR* in Chapter 4, *System Functions and Parameters.*

■ SECURID

The *DYNASTAR* supports SecurID™, a feature that enables only authorized users to access the secured network. The *DYNASTAR* serves as a client to an ACE/Server, requests a user's name and passcode, and communicates that information with the server across a TCP/IP network. The server authenticates the user and responds back to the *DYNASTAR* with an access granted or access denied message.

SecurID supports the following user access protocols:

- X.25 calls directed to the Async Services menu or to the Supervisor Port.
- Telnet-in access to services provided by the *DYNASTAR*, including the Supervisor and PAD ports.
- Asynchronous access at *DYNASTAR* physical PAD ports.

SecurID does not support the following user access protocols:

- IPX-In
- SLIP
- Asynchronous PPP
- Bridged and routed traffic

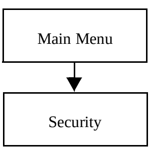
SecurID Features

SecurID's authentication consists of a two-part passcode:

- A user's personal identification number (PIN), known only to the user.
- A current code from the user's SecurID card. The code changes frequently, approximately once every minute.

The two-part passcode provides effective security since access is not granted unless both the PIN and passcode are correctly entered by the user. Therefore, if a PIN is learned or the SecurID card lost, the network cannot be accessed.

Other SecurID features include:



- Slave backup server, a second server that acts as a backup in the event that the primary server fails
- Encrypted communications between the *DynaStar* and the SecurID server, using DES or Security Dynamics proprietary encryption
- Supervisor port management of SecurID
- SNMP access to SecurID configuration information

NOTE: By default, SecurID is disabled and can be enabled on the Console Port of the *DynaStar*.

NOTE: If a secure terminal is directly attached, you can disable SecurID authorization at port 6 to ensure that you can manage the *DynaStar* even if SecurID authorization is not working.

ACE/Server and ACE/Client

SecurID works in a client/server environment. In this environment, the *DynaStar* is always a client on the network (clients can be any type of workstation). Some configuration is needed on both the client and the server for SecurID to be implemented.

The server (and backup slave server) is a UNIX workstation that runs ACE/Server software developed by Security Dynamics. On the server side, you must run the **sdadmin** program to add each *DYNASTAR* client. (See the Security Dynamics *System Administrator's Guide* to configure the ACE/Server to include a *DYNASTAR* as a client.) Certain server configuration items must be synchronized with the client's configuration items. The *DYNASTAR* should be added as a Communication Server client.

You must configure the SecurID feature via the SecurID Access Authorization screen (see Figure 3-22) before you can implement it. Table 3-1 defines the parameters on the SecurID Access Authorization screen.

To set the SecurID parameters:

1. From the Main menu, select **Security**.

✓ The Security Commands menu, shown in Figure 3-21, is displayed.

```
                         ***Security Commands***

1 -  Password Change       Change Operator Password
2 -  Access Security       Change Operator Access
3 -  IPX-In Security       IPX-In ID strings
4 -  IPX-Out security      IPX-Out service restrictions
5 -  IP Filter             IP Address Filter
6 -  TL1 security          Add/Change TL1 Username/Password
7 -  Network security      Add/Change Network Passwords
8 -  Destinations          Add/Change Permitted Destinations
9 -  Security Options      Validation options and methods
10 - SecurID               Access Authorization
11 - Port Selection        Which ports have security enforced

                         Enter command number:

_______[DynaStar dc000345]_______
Terminate input with <RET>.              Press ESC to return to previous menu.
```

Figure 3-21 Security Commands Menu

2. Select the **SecurID** option and press **<return>**.

✓ The SecurID Access Authorization screen appears, as shown in Figure 3-22.

3. Configure the following items to agree with the configuration of the ACE/Server:

- DES encryption
- Authentication service name
- Authentication service port number
- Master Server name and IP address
- Enabling of a Slave Server
- Slave Server name and IP address (if slave server is used)

4. Configure other items as appropriate for your network.

5. When you have completed your configuration, enter **Y** in the **Process selections** field and press **<return>**.

✓ Your entries are processed and you return to the Security Commands menu.

```
***SecurID Access Authorization***

***THIS CONFIGURATION MUST AGREE WITH ACE/SERVER sdconf.rec FILE***
                                                         Last changed: 4-24-02 22:00:33
SecurID feature: [Disabled]                              Disabled
Authorize console (Port 6) accesses: (Y/N)?[N]           N
Logging of authorizations & denials (Y/N)?[N]            N
DES encryption: [Disabled]                               Disabled
Audit Trail Traps (Y/N)? [N]                             N
User Interface Characteristics
  Retry attempts before disconnect (0-5):[0]             0
  Baseline delay between accesses (0-10 sec): [2]        2
  Increasing delay with failures [Y/N]  [N]              N
ACE/Server Interface Characteristics
  Authentication service name: [securid]                 securid   (15)
  Authentication service port number: [5500]             5500
  Retry attempts (1-6): [5]                              0
  Retry interval (1-20 sec): [5]                         5
  Clear Node Secret: (Y/N):  [N]                         N
Master Server                   Slave Server             Disabled
  Server name:          (15)        Server name:             (15)
  IP address: 0.0.0.0                IP address: 0.0.0.0

_______DynaStar_623e_______                         Process selections (Y/N): Y
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 3-22 SecurID Access Authorization Screen

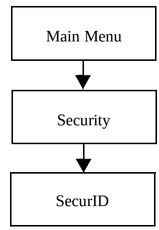


Table 3-1 SecurID Access Authorization Parameters

Parameter	Meaning	Settings
SecurID feature	Enables or disables SecurID for all async access protocols.	Enabled Disabled (default)
Authorize console (Port 6) accesses	If SecurID is enabled, setting this option to Y enables SecurID on the console port. Set this option to N to allow a “back door” for accessing service menus.	Y, N (default)
Logging of authorizations and denials	If set to Y, a log entry is made every time an attempt is made to access the device. In addition to information typically available in the server’s log, the message tells which port the attempt was made on and what service was being accessed.	Y, N (default)
DES encryption	In the standard product version, this option is not available. In units with DES, encryption can be enabled/disabled. This setting must agree with the server setting. See the next section, *SecurID Software Versions*, for additional information.	Enabled Disabled (default)
Retry attempts before disconnect	Number of times a user can reattempt access after being denied. When the limit is reached, the port is disconnected.	0-5 Default = 0
Baseline delay between accesses	Delay between *Access denied message* and the *Enter username message* that permits the next attempt.	0-10 seconds Default = 2

Table 3-1 SecurID Access Authorization Parameters (cont.)

Parameter	Meaning	Settings
Increasing delay with failures	If this option is set to N, the delay between access attempts is a constant. If the option is set toY, the delay doubles after each denial.	Y, N (default)
Authentication service name	Name you are using on this network for the SecurID service. This name must match the name in the */etc/services* file on the ACE/Server.	Default = securid
Authentication service port number	UDP Port # used for the SecurID service. Must agree with ACE/Server setting.	Default = 5500
Retry attempts	The number of times the *DYNASTAR* attempts to reach the ACE/Server before declaring failure. Must agree with ACE/Server setting.	1-6 Default = 5
Retry interval	Number of seconds between attempts to reach the ACE/Server. Must agree with ACE/Server setting.	1-20 seconds Default = 5
Clear Node Secret	When set to Y, clears the existing node secret in the *DYNASTAR* client. This allows a new node secret to be established successfully for an existing *DYNASTAR* (ACE client) and for communication to be successfully reestablished with the ACE Server.	Y/N Default = N
Master Server: Server name	Name of master ACE/Server to which the *DYNASTAR* is connected (15 characters, maximum).	User entry No default
Master Server: IP address	IP address of the master ACE/Server.	User entry No default

Table 3-1 SecurID Access Authorization Parameters (cont.)

Parameter	Meaning	Settings
Slave Server: Enable/Disable	Determines whether the *DynaStar* looks for a Slave ACE/Server if the master fails.	Enabled Disabled (default)
Slave Server: Server name	Name of slave ACE/Server (15 characters, maximum).	User entry No default
Slave Server: IP address	IP address for slave ACE/Server.	User entry No default

SecurID Software Versions

There are two versions of the *DynaStar* SecurID software. The standard version does not include the DES encryption algorithms and may be shipped anywhere in the world. The DES version is only shipped to those customers within the United States who specifically request it. This version includes both the DES and the proprietary Security Dynamics encryption algorithms and may not be exported from the United States by the customer.

SecurID Login Instructions

To access the network, a user must enter a valid username and passcode from a standard SecurID passcard or from a SecurID PINPAD card at the *DynaStar* client's secured interface.

1. When prompted, enter your username.
2. When prompted, enter the PIN (up to eight digits) plus the passcode (leave no space between the PIN and passcode).

3. Press **<return>**.

✓ If the PIN and passcode are valid, access is authorized.

NOTE: Refer to the *Authentication* section for information on *Access denied* and other messages.

AUTHENTICATION

When you log in, the *DYNASTAR* will respond with one of the following messages:

- *Passcode accepted.* You have correctly entered the PIN and passcode and are presented with the appropriate screen for the requested service.
- *Access denied.* You have incorrectly entered the PIN and/or the passcode. (Your SecurID token may also have been disabled, either through misuse or by the system administrator.) The prompt screen redisplays up to the maximum number of times specified in the SecurID Access Authorization screen.

NOTE: If you logged in remotely, you are disconnected before further attempts are allowed.

NOTE: If specified in the SecurID Access Authorization screen, time delays increase between access attempts. Note also that the system may request the next passcode or invalidate a passcode.

- *Please enter the next code from your card.* You must enter the next tokencode/passcode displayed on the passcard. This either resynchronizes the server and your passcode or foils someone who may have learned a PIN and is attempting to guess the passcode.
- *New PIN.* If you are a new user or must select a new PIN, you are presented with one of the following messages (depending on your system configuration):

  Enter your new PIN, containing 4 to 8 characters
  OR
  <Return> to generate a new PIN and display it.

The following option is always displayed:

<Ctrl-d> to cancel the New PIN procedure.

The procedure for entering a new PIN is explained in the next section.

NOTE: If you select the option to generate and display a new PIN, the new PIN is displayed for 10 seconds and then erased.

- *PIN Rejected.* The PIN you entered is invalid, and you must repeat the login process as well as the process for your new PIN.

NOTE: If access is denied, your connection is not immediately broken. Instead, there is a delay, after which you are prompted to enter the username and allowed to try again. To discourage unauthorized users, the delay can be configured as fixed, or it can be doubled each time access is denied.

ENTERING A NEW PIN. If the authentication process asks you to enter a new PIN:

1. After you see the new PIN message, press **<return>** to generate a new PIN and display it on the screen.
2. Enter your new 4-to-8-digit PIN.
3. For verification purposes, reenter your new PIN.

   NOTE: To cancel the new PIN operation at any point in the procedure, press **<CTRL-D>**.

■ PORT ACCESS SECURITY

Additional security can be provided by restricting certain users to one or more destinations reached by using mnemonics (destination names). This protects the network as no user can determine the network architecture and users can only contact the approved destinations. Networks can also continue to operate in the absence of a SecurID server.

When a user connects to the system, either via Telnet or a PAD port or modem, he is presented with a locally generated security access banner that is followed by a prompt for a destination. At this point, the user must actually enter his user name and password (the prompt for a destination is deliberately ambiguous). If the user name and password match the configured Names table, the user is prompted again for a destination. At this point, the user enter a mnemonic or type **H** for a list of permitted destinations. The user can subsequently reach other destinations without reentering his name/password.

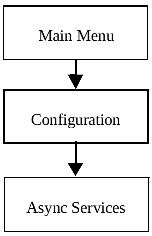
The basic steps in configuring port access security are listed below. More detailed information is given in the sections that follow.

1. Define physical async ports, X.25 routing destinations, and/or IP addresses. (See *Port and Mnemonic Configuration*.)
2. Configure the mnemonics table. (See *Port and Mnemonic Configuration*.)
3. Disable normal Telnet access entry screen. (See *Telnet Access*.)
4. Define user names and passwords. (See *User Names and Passwords*.)
5. Associate mnemonics to user names. (See *Mnemonics*.)
6. Define password and other security options. (See *Security Options*.)
7. Define SecurID parameters if required. (See *SecurID Parameters*.)
8. Define the ports that will be used for access security. (See *Port Security*.)

PORT AND MNEMONIC CONFIGURATION

To implement port access security, you must first configure the physical async ports, X.25 routing destinations, and/or IP addresses.

- Physical async port configuration is discussed in Chapter 7, *The PAD Function*.
- X.25 routing configuration is discussed in Chapter 6, *The X.25 Application*.
- Configuration of the IP addresses for the X25-IN logical ports that support IP Telnet sessions to IP addresses on the local LAN or connected IP network is discussed in Chapter 13, *Telnet and Async Services.*



You must then define the menmonics that will be used for port access security. The mnemonics table associates the addresses that you defined in the step(s) above with a mnemonic. Mnemonics configuration is discussed in Chapter 7, *The PAD Function.*

TELNET ACCESS

Under normal circumstances, when a user accesses the *DYNASTAR* via Telnet, an interim selection menu is displayed. This menu allows the user to connect to the Configuration menu or select a regular async PAD destination. This menu should be bypassed for greater security protection.

To bypass this interim selection menu you must define an async service of type PAD for the console:

1. From the Main menu, select **Configuration**.

✓ The Configuration commands menu (Figure 3-11) appears.

2. From the Configuration menu, select **Async services**.

✓ Ths Access Server Commands menu (Figure 3-23) appears.

3. Select **Async services**.

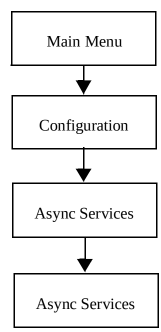
✓ The Async Service Names menu (Figure 3-24) appears.

```
                      ***Access Server Commands***

 1 -  PAD configuration options
 2 -  PAD profiles
 3 -  X.25 Mnemonics
 4 -  NUIs
 5 -  Async services        <PAD, Telnet, IPX-In, SLIP)
 6 -  Logoff scripts
 7 -  EPOS profiles
 8 -  Logon screen          <Initial user screen>
 9 -  Multicast configuration



                         Enter command number:


_______[DynaStar dc000345]_______
Terminate input with <RET>.              Press ESC to return to previous menu.
```

Figure 3-23 Access Server Commands Menu

```
                        *** Async Service Names ***
                                        Last changed: 5-31-02 8:26:38

1-Console
2-Chicago
3-Reading
4-Columbus
5-Great Falls
6-Burbank
7-Omaha
8-
9-
10-
11-
12-
13-
14-
15-
16-

                        Enter service number: 1

_________[DynaStar_3df2]__________
To add entry, just press <RET>.              Press ESC to return to previous menu.
To edit entry, enter service # <RET>.        Cursor up/down for more entries
To delete entry, enter service # <CNTL-D>.   Note: delete takes place immediately.
```

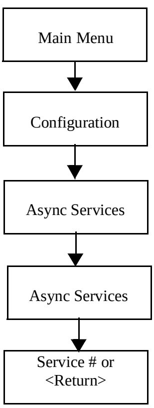
Figure 3-24 Async Service Names Menu



4. Enter the number for the console.

✓ The Async Services menu (Figure 3-25) appears.

CAUTION: If the interim menu is bypassed as described above *and* Secure Access is activated, you ***must*** make sure that a mnemonic has been set up that provides access to the console port and that a user has been defined with access rights to this console mnemonic (see *Mnemonics* below). If this is not done, it will not be possible to access the supervisor port.




```
                         *** Async Services ***

         Service name:          CONSOLE                      (15)
         Service type:          PAD
         IP Address             0.0.0.0
         Socket Number:         23
         X.121 address:                                  (15 BCD)
         X.3 Profile:           87 (12) TELNET          (Name or #)
         Telnet command:                                     (23)
         CUG:                                              (0-99)
         Call UserData:                                      (32)
         TCP Idle Timer:        0                (1-255 min., 0=OFF)

_________[DynaStar_3df2]__________         Process selections (Y/N): Y
Use <CTRL-D> to delete entry.             <RET> to toggle or type value
Use TAB & CURSOR keys to move fields.     Press ESC to return to previous menu
```

Figure 3-25 The Async Services Menu

5. Change the service type to **PAD**.

6. Enter **Y** in the **Process selections** field and press **<return>**.

User Names and Passwords

The Network User Information table lets you enter user names and passwords. These are the users that will be allowed to access the mnemonic destinations. When a new entry is added to the table, a flag is set that forces the user to enter a new password the first time that he logs on to the network. This allows the network administrator to set up a group of new users with temporary passwords, but the users will be forced to assign their own passwords the first time they access the network. You can also set password options and password aging parameters (see *Security Options* below).

1. From the Main menu, select **Security**.

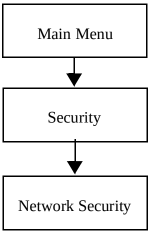
✓ The Security Commands menu appears (Figure 3-15).

2. From the Security Commands menu, select **Network Security**.

✓ The Network Security Information screen (Figure 3-26) appears.

```
                         *** Network Security Information ***
                                          Last changed: 6-5-02 13:24:33

           User Name                      Password
           (16 Chars Max)                 (16 Chars Max)
1          BOB                            Password Accepted
2          TRAVIS                         Password Required
3          WENDY                          Password Accepted









_________[DynaStar_3df2]__________             Process selections (Y/N): Y
Use <CTRL-D> to delete entry.           <RET> to toggle or type value
                                        Press ESC to return to previous menu
```

Figure 3-26 Network Security Information Screen



3. Enter the user name and press **<return>**.

✓ The cursor moves to the Password field, and *Password Required* is displayed.

4. Enter a password.

✓ The *Re-enter password* prompt is displayed.

5. Re-enter the password and press **<return>**.

6. Repeat steps 3 through 5 to enter other user names and passwords.

7. When you have completed your configuration, enter **Y** in the **Process selections** field and press **<return>**.

MNEMONICS

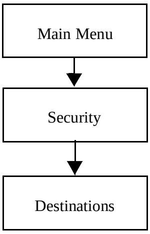
You now need to associate the defined users with the mnemonic destinations that they are allowed to access.

1. From the Main menu, select **Security**.

✓ The Security Commands menu appears (Figure 3-15).

2. From the Security Menu, select **Destinations**.

✓ The User Directory screen (Figure 3-27) appears. This is a read-only list of the configured users in alphabetical order.

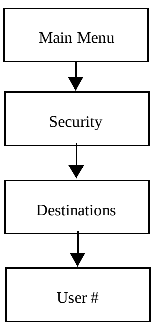



```
                         *** User Directory ***
                                   Last changed: 6-5-02 13:24:33

        1 - BOB
        2 - TRAVIS
        3 - WENDY

                        Enter command number:

_________[DynaStar_3df2]__________
To add entry, just press <RET>              Press ESC to return to previous menu
To edit entry, enter service # <RET>        Cursor up/down for more entries
To delete entry, enter service # CNTL-D     NOTE: delete takes place immediately
```

Figure 3-27 User Directory Screen

3. Enter the number of the user whose destinations you want to define.

✓ The User Permitted Destinations screen (Figure 3-28) appears. This screen automatically lists the destinations from the mnemonics table.




```
                         *** User Permitted Destinations ***
                                               Last changed: 6-5-02 13:24:33

              Destinations                     Permitted
1:            Console                          N
2:            WASH_5E                          N
3:            PHILLY_CS                        Y



                              User Name: BOB


 _________[DynaStar_3df2]__________           Process selections (Y/N): Y
 Use <CTRL-D> to delete entry             <RET> to toggle or type value
 Use <TAB> and CURSOR to move fields      Press ESC to return to previous menu
```

Figure 3-28 User Destination Screen

4. Toggle the *Permitted* field to **N** or **Y** as required and then tab to the next destination. (By default, all destinations are set to *N*.)
5. When you have completed your configuration, enter **Y** at the **Process selections** prompt.
6. To configure additional user names, enter the name at the **User Name** prompt and repeat steps 4 and 5.

Security Options

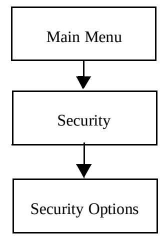
The Security Options menu lets you configure various security options.

1. From the Main menu, select **Security**.

✓ The Security Commands menu appears (Figure 3-15).

2. From the Security Menu, select **Security Options**.

✓ The Security Options menu (Figure 3-29) appears.




```
*** Security Options ***

Local User Validation:          N
Local Console Validation:       N
Remove Validation:              None
Emergency Password:             N
Pasword Aging:                  None          (0-255 days)
User Expiration:                0
Enforce Secure Passwords:       N             (0, 1-30 Min)
User Timeout:                   0



_________[DynaStar_3df2]__________          Process selections (Y/N): Y
<RET> to toggle or type value        Use <TAB> and CURSOR to move fields
Press ESC to return to previous menu
```

Figure 3-29 Security Options Screen

3. Enter values as required. The fields are explained in Table 3-2.
4. When you have completed your configuration, enter **Y** in the **Process selections** field and press **<return>**.

Table 3-2 Security Options

Parameter	Meaning	Settings
Local User Validation	Require users connecting to the *DYNASTAR* to present a valid username and password. Users can be directly connecting to physical ports or remotely accessing via Telnet.	Y N (default)
Local Console Validation	Require users connecting via port 6 to present a valid username and password.	Y N (default)

Table 3-2 Security Options (cont.)

Parameter	Meaning	Settings
Remote Validation	Indicates if SecurID validation is required (mirrors selection from SecurID screen).	None (default) SecurID
Emergency Password	If implemented, provides emergency access to the console if the password is lost. The password can be obtained by calling customer service and providing the MAC address of the device. The password given is good for one access to the device.	Y N (default)
Password Aging	Time after which the user must change his password.	None (default) 30 days 60 days 90 days
User Expiration	If a user has not used his account for this number of days, the account will be disabled.	0 -255 days 0 = default (0 = never disable)
Enforce Secure Passwords	Forces the user to select a password of at least 8 characters, with at least one alphabetic and one numeric character.	Y N (default)
User Timeout	Inactive calls are cleared after this amount of time. This value applies to all users of the system.	0 (default) 1 - 30 minutes (0 = disabled)

SecurID Parameters

If SecurID will be used as an additional security measure, the parameters should be defined now. See *SecurID* earlier in this chapter.

Port Security

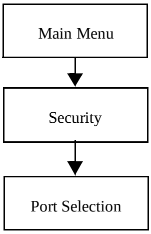
You now need to indicate which ports are participating in port security.

1. From the Main menu, select **Security**.

✓ The Security Commands menu (Figure 3-17) appears.

2. From the Security Commands menu, select **Port Selection**.

✓ The Port Security screen (Figure 3-30) appears. This screen indicates whether or not local security or SecurID is enabled. If *Local* is set to **Y**, then a user-name and password must be entered before users on that port will be allowed to connect to the *DynaStar*. If *SecurID* is set to **Y**, then SecurID server and tokens must be presented before users on that port will be allowed to connect to the *DynaStar*. Each port can be set for *Local* and/or *SecurID*.




```
                    *** Port Security Menu  ***

Port    Name                Local      SecurID
0       Ethernet            N          N
1       QUAD card           N          N
2       Unmanaged 10BaseT   N          N
3       Sync/Async          N          N
4       CSU/DSU chan 1      N          N
5       CSU/DSU chan 2      N          N
6       Console             N          N
10      Virtual PAD         N          N
11      CSU/DSU trunk 1     N          N
12      CSU/DSU trunk 2     N          N
99      Virtual X.25        N          N

_________[DynaStar_3df2]__________          Process selections (Y/N): Y
<RET> to toggle or type value           Press ESC to return to previous menu
Press <CTRL-O> to configure separately.     Cursor up/down for more entries.
```

Figure 3-30 Port Security Screen

3. Configure the screen as required. In most cases, the port number represents the actual physical port on the DYNASTAR. Port 10 represents all inbound Telnet sessiona, and port 99 represents virtual X.25 ports used in tunneling X.25 over Frame Relay. To separately configure ports on a multi-port card (for example, the QUAD card), type <CTRL-O> and a screen will appear listing the individual ports.
4. When you have completed your configuration, enter **Y** in the **Process selections** field and press **<return>**.

LOGON SCREEN

If desired, you can configure a security warning page that is displayed when the user logs on. If configured, this page is displayed regardless of whether other security features are enabled.

1. From the Main menu, select **Configuration**.

✓ The Configuration menu (Figure 3-11) appears.

2. From the Configuration menu, select **Async Services**.

✓ The Access Server Commands menu appears (Figure 3-23).

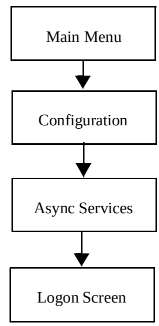
3. From the Access Server Commands menu, select **Logon Screen**.

✓ The Logon Screen (Figure 3-31) appears.

4. Enter your logon text. You can enter up to 30 lines of text with a maximum of 75 characters each.
5. When you have completed your configuration, enter **Y** in the **Process selections** field and press **<return>**.

```
*** Logon Screen ***
                                        Last changed: 06-05-02

   Enter Text, Spaces Permitted
   (75 Chars Max)
1         DYMEC-DynaStar
2
3  Unauthorized Use of This System Is Prohibited

_________[DynaStar_3df2]__________        Process selections (Y/N): Y
Use <CTRL-D> to delete entry        Press ESC to return to previous menu
```

Figure 3-31 Logon Screen



■ LAN SECURITY

The following security options are available:

- PAP/CHAP. For more information, see Chapter 10, *The PPP Application*.
- IP filtering. For more information, see Chapter 12, *The IP/IPX Router Application*.

■ VPN SECURITY

The *DYNASTAR* offers VPN (Virtual Private Network) implementation as an optional software feature. The *DYNASTAR* implementation of a VPN conforms to IPSec RFC2401. IPSec (IP Security) provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and set up any cryptographic keys required to provide the requested services. IPSec can be used to protect one or more "paths" between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

For more information on the configuration and use of VPNs in your *DYNASTAR* network, see Chapter 12, *The IP/IPX Router Application.*

SYSTEM FUNCTIONS AND PARAMETERS

■ OVERVIEW

This chapter covers the following functions that affect the *DYNASTAR* as a unit:

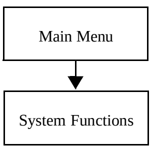
- Setting the system date and time
- Activating or deactivating an application
- Restarting the system
- Enabling and disabling ports
- Busying and unbusying ports
- Initializing ports
- Setting systemwide parameters such as certain timers
- Updating system software
- Uploading/downloading *DYNASTAR* configuration files

■ SYSTEM COMMANDS

System functions accessed from the Systems Commands menu include setting the date and time, activating applications, uploading or downloading code, and restarting the unit. To access the System Commands menu:

1. From the Main menu, select **System Functions**.

✓ The menu shown in Figure 4-1 is displayed.




```
                    ***System Commands***

1 -  Date & Time        Set the system date and/or time
2 -  Applications       Activate applications and check versions
3 -  Load code          Update system software
4 -  Warm restart       Restart system
5 -  Cold restart       Restart system & reset config to default values
6 -  Reinitialize       Restart system & reset config from cnfgload.cmp
7 -  Code versions      Display downloaded software versions


                    Enter command number:


_______[DynaStar dc000345]_______
Terminate input with <RET>.          Press ESC to return to previous menu.
```

Figure 4-1 System Commands Menu

SETTING THE SYSTEM'S DATE AND TIME

To set the system date or time:

1. From the Main menu, select **System Functions**.

✓ The System Commands menu (Figure 4-1) is displayed.

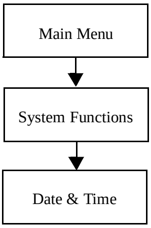
2. Select **Date & Time**.

✓ The System Date & Time menu (Figure 4-2) is displayed. The date format is mm/dd/yy. The time is given using a 24-hour clock. The default time is 00:00:00.

3. Make any changes necessary.

4. In the **Process new date and time** field, enter **Y** and press **<return>**.

✓ You return to the System Commands menu.




```
*** Change System Date & Time ***

Current Date          month:    5     (1 - 12)
                        day:    2     (1 - 31)
                       year:   02     (95 - 53)

Current Time           hour:   17     (0 - 23)
                     minute:   43     (0 - 59)
                     second:   32     (0 - 59)

                                Process new date and time (Y/N): Y
________[DynaStar_3df2]__________
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 4-2 System Date and Time Menu

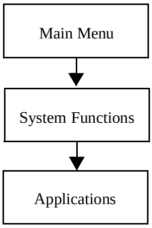
ACTIVATING OR DEACTIVATING AN APPLICATION

The *DYNASTAR* has a number of independent applications stored in EEPROM. All *DYNASTARS* are shipped with Router, X.25, Frame Relay, and Network Management applications activated. In addition, you can configure the *DYNASTAR* to support the additional applications such as Access Server, Bridge, X.25 switch, OSI.Gate, and compression.

On the *DYNASTAR 500* and *DYNASTAR 5000*, you can also activate external temperature and power alarms.

NOTE: When you activate an application, port parameters *are not* automatically set to new values. You *must* check port parameters and adjust applicable values.

The Applications menu (Figure 4-3) lists the code that is loaded into the *DYNASTAR* as well as the optional applications that are present on the EEPROM. These optional applications are followed by an indication of whether the application is



activated (Y, N, Limited, or Full). The bottom of the screen contains fields that let you enable the power supply and temperature alarms. These fields are labeled *Auxiliary Functions*.

```
                              *** Applications ***

Serial Number:      3df2     ROM Installed: 3.9    NCSI_WAN Required:   3.2
Private MIB Version: 4.2     ROM Required:  3.9    INT14WAN Required:   1.0
                              X.25 Version:  2.0    OSI Version:         1.00

File            Date     Time  Blocks  File          Date      Time  Blocks
DOWNLOAD.BIN*10-09-02 11:27 3973    ATICLOAD.BIN  <not loaded>
ETH8LOAD.BIN  10-09-02 11:27  174    QPMLOAD.BIN   <not loaded>
DMAPLOAD.BIN  10-09-02 11:27  196    No binary config file loaded
QUADLOAD.BIN  10-09-02 11:27  333
816PLOAD.BIN  10-09-02 11:27  319
T1E1LOAD.BIN  10-09-02 11:27  331
DBRILOAD.BIN  10-09-02 11:27  278
  * running version      5253 KB free
                              Toggle with <RET>      Type in value
                                  -------------         -------------
DynaStar OSI.Gate Application         Limited

Auxiliary Functions                  Temp                  Save Setting
                                     Sensor                when Exit
Active (Y/N):                          N                      N


_________[DynaStar_3df2]__________
Use TAB & CURSOR keys to move among fields. Press ESC to return to previous menu.
```

Figure 4-3 Typical Applications Menu

To activate or deactivate an application on the *DYNASTAR*:

1. From the Main menu, select **System Functions**.
2. The System Commands menu (Figure 4-1) is displayed.
3. Select **Applications**.

✓ The Applications menu (Figure 4-3) is displayed.

4. Where applicable, select **Y** to activate an application or function or **N** to deactivate it.

✓ The message **Are you sure? (Y/N)** appears to the right of the application.

NOTE: Some applications, such as OSI.Gate, will indicate **Limited** or **Full** and expect you to enter a license key.

5. Enter **Y** to confirm your change, or **N** to negate it.
6. When you are finished activating/deactivating applications, press **<ESC>** to return to the previous menu.

To activate or deactivate the auxiliary functions:

1. Move the cursor to the field you want to activate or deactivate and select **Y** to activate or **N** to deactivate.
2. Move the cursor to the **Save Setting** field and select **Y** to save your selections.
3. Press **<ESC>** to return to the previous menu.

WAYS TO RESTART THE SYSTEM

There are three commands on the System Commands menu (Figure 4-1) for restarting the system: Warm restart, Cold restart, and Reinitialize.

- A *warm restart* is equivalent to powering the *DYNASTAR* off and on. Configuration parameters are not affected. If two operating systems are available on your unit, you will be asked which one to use.

CAUTION: If you have not saved your changes to flash memory while configuring the *DYNASTAR*, use the CTRL-W command to save them before warm starting the unit.

- A *cold restart* is equivalent to powering the *DYNASTAR* off, removing the CLR CONFIG jumper located on the baseboard, and powering the system back on. Configuration parameters revert to default values.

CAUTION: When parameters are reset to defaults, you may lose access to the server from the Supervisor Console port.

- *Reinitializing* the *DYNASTAR* reloads the compressed configuration file, **cnfgload.cmp**, from flash memory. When you have downloaded a configuration file, this command is required to reset *DYNASTAR* parameters to the values contained in the downloaded file. The configuration file is present in flash only if it has been uploaded or downloaded previously. The *DYNASTAR* creates the file when it receives a valid TFTP *GET* command to upload the file. If the file has

been erased, it can be restored from a remote archive using the TFTP *PUT* command. See the section *Updating System Software* later in this chapter.

NOTE: An equivalent reinitialization command is available for TFTP transfers. For examples of its use, see *Updating System Software* later in this chapter.

CAUTION: If there is no configuration file stored in flash memory, reinitialization resets all parameters to default, just like a cold restart, and can cause you to lose remote access to the Console port.

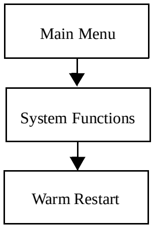
NOTE: An individual port can be initialized without restarting the *DYNASTAR*. For more information, see the section *Initializing Ports* later in this chapter.

RESTARTING THE *DYNASTAR*. To perform a restart:

1. From the Main menu, select **System Functions**.

✓ The System Commands menu (Figure 4-1) is displayed.

2. Select **Warm restart** if you want to restart the *DYNASTAR* and all its ports and maintain current parameter settings.

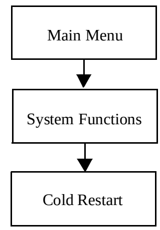



```
                         *** Warm Restart ***



  Press <CTRl-O> to select software version:

              6.07 (RC43)
         *    6.08 (RC49)



         Enter Current Password: ________________




________[DynaStar_3df2]__________
Terminate input with <RET>            Press ESC to abort command & exit.
```

Figure 4-4 Warm Restart Menu

- ✓ The Warm Restart menu (Figure 4-4) is displayed. If two operating systems are available, you must select which one to use.
  OR
  Select **Cold restart** if you want to restart the *DYNASTAR* and all of its ports and return all parameters to their default settings.

- ✓ The Cold Restart menu (Figure 4-5) is displayed.




```
                              *** Cold Restart ***



WARNING:     All configuration parameters will be reset to default values.
             You may lose access to the Server from your supervisor console.


             Enter Current Password: ________________







 _________[DynaStar_3df2]__________
 Terminate input with <RET>.              Press ESC to abort command & exit.
```

Figure 4-5 Cold Restart Menu

3. Enter the current system password in the field provided and press **<return>**.

- ✓ The system is immediately restarted. All calls are disconnected. System tests are performed. When the restart is complete, the Login screen is displayed. If you have performed a cold restart, all parameters are reset to their default values.
  OR
  Press **<ESC>** to abort the restart.

- ✓ You return to the System Commands menu (Figure 4-1).

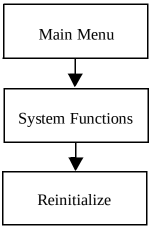
REINITIALIZING THE *DYNASTAR*. The reinitialization command loads the compressed configuration file **cnfgload.cmp** from flash memory if the file is present; otherwise, it cold starts the unit. To reinitialize the unit:

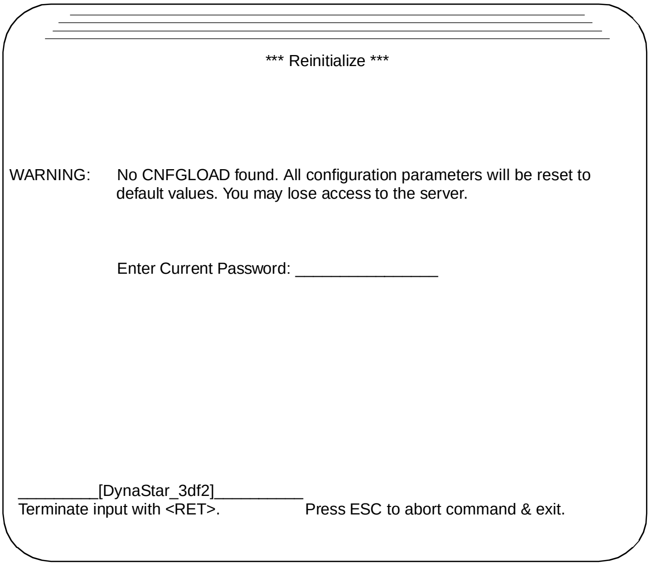
1. From the Main menu, select **System Functions**.

✓ The System Commands menu (Figure 4-1) is displayed.

2. Select **Reinitialize**.

✓ The Reinitialize menu (Figure 4-6) is displayed. The message “All configuration parameters will be set from CNFGLOAD.CMP” may appear if you have loaded a compressed configuration file into the unit. See the previous section, *Ways to Restart the System*, for more information.





*** Reinitialize ***

WARNING: No CNFGLOAD found. All configuration parameters will be reset to default values. You may lose access to the server.

Enter Current Password: ________________

_________[DynaStar_3df2]__________
Terminate input with <RET>. Press ESC to abort command & exit.

Figure 4-6 Reinitialize Menu (no current config file)

3. Enter the current system password in the field provided and press **<return>**.

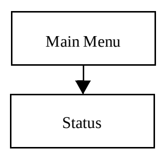
✓ The *DYNASTAR* parameters are set to the values contained in the compressed configuration file.

■ TAKING PORTS OUT OF SERVICE

There are two methods for taking *DYNASTAR* ports out of service from the Supervisor Console. The **Disable Port** command clears any calls in progress and blocks the port until it is placed in service with the **Enable Port** command.

For an X.25 port, you can use the **Busy** command to gracefully place the port out of service. Any calls using the port at the time the **Busy** command is executed are not affected. However, new incoming calls are refused and the port is not allowed to originate calls. When existing calls terminate, you can perform maintenance on the port without disrupting callers. The **Unbusy** command returns the port to service.

CHECKING PORT STATUS



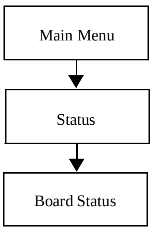
You can check the Board Status menu to see if a port has been placed out of service. To access the Board Status menu:

1. From the Main menu, select **Status**.

✓ The Status Commands menu (Figure 4-7) is displayed.

```
                              *** Status Commands ***


1 -  Board Status              Display internal module types and status
2 -  Call status               Check call status and manually disconnect calls
3 -  Names/Addresses           Verify names & MAC, IP, IPX and X.121 addresses
4 -  Statistics                Show statistics for port n
5 -  Buffer Usage              System buffer usage
6 -  Disable Port              Put port n in Disabled state (busy out dial ports)
7 -  Enable Port               Bring port n to an Enabled state
8 -  Initialize Port           Perform initialization on port n
9 -  Log                       Display system error log
10 - Monitoring                Show input/output data packets for port n
11 - Busy/UnBusy Port          Bring port n to Busy/UnBusy state
12 - PPP status                Check call status
13 - OSI                       OSI operator console
14 - Modem Status              Show statistics & status for modem resources
15 - Call History              Show status of transactions per ISDN port
16 - Trace                     SNA Trace

                               Enter command number:

_________[DynaStar_3df2]__________
Terminate input with <RET>.              Press ESC to return to previous menu.
```

Figure 4-7   Status Commands Menu



2. Select **Board Status**.

✓ The Board Status menu (Figure 4-8) is displayed. The status and state of each port is listed. If the port has been disabled, its status will be **Disabled**. If a port has been made busy, its state will be **Busy**. For information on the Board Status menu, see Chapter 19, *Monitoring and Statistics*.

```
                              *** Board Status ***
DynaStar100e                                                       5-22-02 16:51:55

                Ethernet        SLOT 1          SLOT 2
Port number:    0               101-104         201-214
Name:           Ethernet        IS-QUAD         UnmEther SW
Interface:      IS-Enet
Protocol:       ethernet
State:          Enabled
Status:         Up

                Sync/Async      T1 CSU 1         T1 CSU2          Console
Port number:    3               4                5                6
Name:           Sync/Async      CSU/DSU chan 1   CSU/DSU chan 2   Console
Interface:      RS-232          TDM channel      TDM channel      RS-232
Protocol:       PPP             X.25 line        X.25 line        console
State:          Enabled         Enabled          Enabled          Enabled
Status:         Up              Up               Up               Up - 1
Alarm State:                    No alarms        No alarms
                 Enter slot # to view status of multiple port module:


_________[DynaStar_3df2]__________            Press <RET> for upcate
                                               Press ESC to return to previous menu.
```

Figure 4-8 Typical *DYNASTAR* Board Status Menu

DISABLE PORT

Use the **Disable Port** command to immediately put a port out of service and clear any existing calls on the port.

CAUTION: If you disable the asynchronous port to which your Supervisor Console is attached, you will have to access the Supervisor through another means to enable the port. However, you can initialize the port without losing the Supervisor Console connection. See the section *Initializing Ports* later in this chapter.

CAUTION: Never disable all ports on the *DYNASTAR*. If you do, you will lose all configured parameter settings in regaining access to the ports. Refer to the *Clear Configuration* section in Chapter 2 or Chapter 3 for more information.

To put a port out of service:

1. From the Main menu, select **Status**.

✓ The Status Commands menu (Figure 4-7) is displayed.

2. Select **Disable Port**.

✓ The Disable Port menu (Figure 4-9) is displayed.

3. In the field **Enter port number**, enter the number of the port you want to disable and press **<return>**.

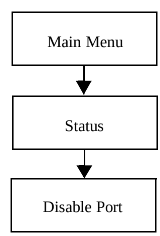
✓ The prompt **Process disable selections** appears on the screen.

4. To disable the selected port, enter **Y** and press **<return>**.

✓ The port is immediately disabled.

```
                         *** Disable Port ***


Valid port numbers (with names) are:
 0: Ethernet
 1: HS 8-port card
 2: 16-port card
 4: ATM slot 4
 5: Dual T1/E1
 6: Console
 7: Sync/Async
 8: HS WAN 1
 9: HS WAN 2
10: Virtual PAD
99: Virtual X.25 Ports


                              Enter port number:


_________[DynaStar_3df2]__________
Terminate input with <RET>.              Press ESC to return to previous menu.
```

Figure 4-9 Typical Disable Port Menu



ENABLE PORT

To enable a port that has been disabled:

1. From the Main menu, select **Status**.

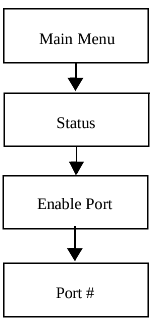
✓ The Status Commands menu (Figure 4-7) is displayed.

2. Select **Enable Port**.

✓ The Enable Port menu (Figure 4-10) is displayed.

3. In the field **Enter port number**, enter the number of the port you want to enable.

✓ The message *Port n enabled* appears on the screen.




```
                              *** Enable Port ***

Valid port numbers (with names) are:
 0: Ethernet
 1: HS 8-port card
 2: 16-port card
 4: ATM slot 4
 5: Dual T1/E1
 6: Console
 7: Sync/Async
 8: HS WAN 1
 9: HS WAN 2
10: Virtual PAD
99: Virtual X.25 Ports

                                        Enter port number:

_________[DynaStar_3df2]__________
Terminate input with <RET>.                 Press ESC to return to previous menu.
```

Figure 4-10 Typical Enable Port Menu

BUSY PORT

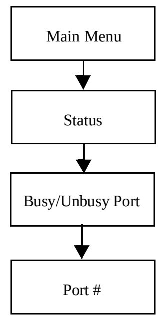
To place an X.25 port out of service gracefully using the **Busy Port** command:

1. From the Main menu, select **Status**.

✓ The Status Commands menu (Figure 4-7) is displayed.

2. Select **Busy/Unbusy Port**.

✓ The Busy/Unbusy Port menu (Figure 4-11) is displayed.




```
                         *** Busy/Unbusy Port ***


Valid port numbers (with names) are:
 0: Ethernet
 1: HS 8-port card
 2: 16-port card
 4: ATM slot 4
 5: Dual T1/E1
 6: Console
 7: Sync/Async
 8: HS WAN 1
 9: HS WAN 2
10: Virtual PAD
99: Virtual X.25 Ports


                                   Enter port number:


_________[DynaStar_3df2]__________
Terminate input with <RET>.                Press ESC to return to previous menu.
```

Figure 4-11 Typical Busy/Unbusy Port Menu

3. In the **Enter port number** field, enter the port number you want to make Busy and press **<return>**.

✓ The message *Port n is made Busy* is displayed. Any calls in progress are not affected. No additional calls are accepted or originated by the port.

Unbusy Port

To make available an X.25 port that has been removed from service with the **Busy** command:

1. From the Main menu, select **Status**.

✓ The Status Commands menu (Figure 4-7) is displayed.

2. Select **Busy/Unbusy Port**.

✓ The Busy/Unbusy Port menu (Figure 4-11) is displayed.

3. In the field **Enter port number**, enter the number of the port you want to return to service and press **<return>**.

✓ The message *Port n is made Unbusy* is displayed and the port becomes available for use.

■ Initializing Ports

All *DynaStar* ports can be individually initialized without restarting the *DynaStar*. When a port is initialized, the port is brought down and back up immediately, any active calls are cleared, the port is configured, and any data strings required to make the port operational are transmitted by the *DynaStar*.

NOTE: Port initialization makes it possible to add an Interface Module to an operational *DynaStar*. This feature also makes it possible to clear a call or reset statistics on any port, including the Supervisor Console port, without losing the connection.

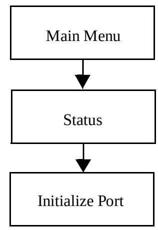
NOTE: It is recommended that you initialize any traffic bearing port after modifying port parameters.

NOTE: The initialize port function has no effect on T1/E1 trunks; however, it can be used for individual channels assigned to these trunks.

To initialize a port:

1. From the Main menu, select **Status**.

✓ The Status Commands menu (Figure 4-7) is displayed.



2. Select **Initialize Port**.

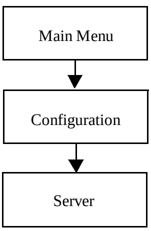
✓ The Initialize Port menu (Figure 4-12) is displayed.

```
                         *** Initialize Port ***

Valid port numbers (with names) are:
 0: Ethernet
 1: HS 8-port card
 2: 16-port card
 4: ATM slot 4
 5: Dual T1/E1
 6: Console
 7: Sync/Async
 8: HS WAN 1
 9: HS WAN 2
10: Virtual PAD
99: Virtual X.25 Ports

                              Enter port number:

_________[DynaStar_3df2]__________
Terminate input with <RET>.                Press ESC to return to previous menu.
```

Figure 4-12 Typical Initialize Port Menu

3. Enter the number of the port you want to initialize in the field provided and press **<return>**.

✓ The port is brought down and back up. If a call is connected, it is cleared. All statistics for the port are reset to zero. If the port was previously made busy, its status becomes unbusy. If a port was previously disabled, it is enabled.



■ SETTING SYSTEMWIDE PARAMETERS

Certain parameters that apply to all *DYNASTAR* ports are set on the Systemwide Parameters screen, shown in Figure 4-13. The parameters are explained in Table 4-1.

```
                         *** Systemwide Parameters***


Server name: DynaStar399c                                                (47)
Supervisor console herald:       DynaStar Supervisor                     (32)
Dial IP idle timer:              2             (0-disable, 1-254 min, 255-10 sec)
Dial IPX idle timer:             2                         (0-disable, 1-255 min)
Dial Bridge idle timer:          2                         (0-disable, 1-255 min)
B Channel call timeout:          0                        (0-disable, 1-1440 min)
X.25 call set-up timer:          5                                   (1-30 min)
XOT Idle Timer                   0                          (0-disable, 1-30 min)
PPP IP prioritization:           0                            (0 - disable, 1-99)
IPX-In preferred File Server:                                            (47)
IPX-Out broadcast address:       399c                                     (8)
Reserved LCNs:                   N                                <CR> to toggle
Exhaustive Routing:              ENDPOINT                         <CR> to toggle
X32 No LCN Drop Timer:           6                    <0-disable, 1-12<10 sec>>
Daughter Board Auto-Recover:     Y                                <CR> to toggle



_______[DynaStar 399c]_______                      Process selections (Y/N): Y
Use <TAB> and CURSOR to move fields.   Press ESC to return to previous menu
```

Figure 4-13 Systemwide Parameters Screen

Table 4-1 Systemwide Parameters

Parameter	Meaning	Values
Server name	Global name assigned to the *DYNASTAR*. The server name appears at the bottom of most *DYNASTAR* menus.	Maximum of 47 characters (no spaces). The name must be unique throughout inter-connected IPX net-works. Default is the *DYNASTAR*'s serial number.

Table 4-1 Systemwide Parameters (cont.)

Parameter	Meaning	Values
Supervisor console herald	Banner that appears on the screen when the user successfully logs in to the Supervisor Console.	Maximum of 32 printable characters. Default is *DYNASTAR* Supervisor.
Dial IP idle timer	If no IP traffic is detected for the number of minutes specified, the call is cleared. Applies to all IP traffic, except RIPs, even if encapsulated. See Chapter 10, *The PPP Application*, for more information.	0-disable 1-254 minutes 255 is interpreted as 10 seconds (allows a value less than 1 minute) Default = 2 [mins]
Dial IPX idle timer	If no IPX traffic is detected for the number of minutes specified, the call is cleared (virtual call if connection is X.25; physical call if connection is ISDN). Applies to all IPX traffic, except RIPs and SAPs, even if encapsulated. See Chapter 10, *The PPP Application*, for more information.	0-disable 1-255 minutes Default = 2
Dial bridge idle timer	If no dial traffic is detected for the number of minutes specified, the call is cleared (virtual call if connection is X.25; physical call if connection is ISDN). Applies to all dial bridge traffic, except spanning tree messages, even if encapsulated. See Chapter 10, *The PPP Application*, for more information.	0-disable 1-255 minutes Default = 2

Table 4-1 Systemwide Parameters (cont.)

Parameter	Meaning	Values
B Channel call time-out	On time-out, disables the entire BRI interface (both B-channels and the D-channel). To reenable the BRI, you must reenable the BRI physical port. Serves as a protection against "runaway" applications. (Does not apply to X.25 calls over the D-channel.) See Chapter 10, *The PPP Application*, for more information.	0-1440 minutes (24 hours) Default=0 (disabled)
X.25 call setup timer	When a call attempt is unsuccessful, the *DYNASTAR* tries to reestablish the call by sending Call Request packets at the frequency defined by the setup timer. Applies to all X.25 bridge and router calls. For more information, see Chapter 6, *The X.25 Application.*	1-30 minutes Default = 5
XOT Idle Timer	If enabled and no traffic is detected on the line for the specified period, the connection is cleared.	0, 1-30 minutes Default = 0 (disabled)
PPP IP prioritization	On a PPP connection, gives priority to data packets with the *DYNASTAR*'s Ethernet IP address as their source address. The value of this parameter determines the number of times the *DYNASTAR*'s data packets will be considered for transmission before other IP traffic is allowed over the connection. When this parameter is set to zero, the *DYNASTAR* traffic receives no preference.	0, 1-99 Default = 0 (disabled)
IPX-In preferred File Server	Novell file server to be logged into by default. For more information, see Chapter 12, *The IP/IPX Router Application.*	Maximum of 47 characters (no spaces) Default = null

Table 4-1 Systemwide Parameters (cont.)

Parameter	Meaning	Values
IPX-Out broadcast address	IPX number that the *DYNASTAR* broadcasts for IPX-Out connection. For more information, see Chapter 12, *The IP/IPX Router Application.*	Maximum of 8 printable characters (no spaces). Default = serial number of the *DYNASTAR*
Reserved LCNs	When this option is on, the first ten entries in the mnemonic table are reserved as priority LCNs. See Chapter 7, *The PAD Function*, for additional information on this parameter.	Y, N Default = N
Exhaustive routing	Toggle to specify how calls are rerouted after a setup attempt fails. Endpoint: Calls can be rerouted back out the trunk they came in on. Privileged: Calls cannot be routed back over the same trunk they came in on. The *DYNASTAR* finds the best valid route and attempts to establish a call. Exhaustive: Calls cannot be routed back over the same trunk they came in on. If a call setup attempt is cleared, the *DYNASTAR* tries each valid route until a call is established or no further routes exist.	Endpoint (Default) Privileged Exhaustive
X32 No LCN Drop Timer	For X.32, the amount of time that can elapse before the call is dropped if there is no LCN.	0 (Disable) 1-12, each representing 10 seconds Default = 6 (that is, 60 seconds)
Daughter Board Auto-Recover	If the daughterboard fails, it will attempt an autorecovery if set toY.	Y, N Default = Y

■ UPDATING SYSTEM SOFTWARE

The flash memory on the *DYNASTAR* contains the DOWNLOAD.BIN file. This file contains subfiles with the software needed to run the various applications and modules on the *DYNASTAR*. These subfiles are listed below:

- ETH8LOAD.BIN: software for the Ethernet switch module
- DMAPLOAD.BIN: DMA controller runtime file for the *DYNASTAR 5000*
- QUADLOAD.BIN: software for a QUAD Interface Module
- ETHERNET.BIN: software for an ENET Interface Module
- ATICLOAD.BIN: software for an ATM Interface Module
- 816PLOAD.BIN: software for an 8-Port or a 16-Port Interface Module
- T1E1LOAD.BIN: software for T1 and E1 PRI Interface Modules
- DBRILOAD.BIN: software for a dual BRI Interface Module
- VRTXOSI1.BIN: software for the OSI.Gate application (installed only if purchased as an option)
- QPM_LOAD.BIN: software for the digital modem subsystem
- CNFGLOAD.CMP: compressed configuration file from a previous software version. This file is not always present in flash memory. It is created when a valid TFTP *get* request is issued to the *DYNASTAR*.

CAUTION: To retain old configuration information as you update system software, you must load CNFGLOAD.CMP along with other system modules. For more information, see the section *Compressed Configuration File*.

NOTE: There is no special software file for the OCTAL+ Interface Module.

From time to time, *DYMEC-DYNASTAR* may make changes in the system software. New versions of software are distributed on a *DYNASTAR* software diskette that contains a file with the filename format of DOWNLOAD.*xxx* (for the *DYNASTAR 100, 100i,* and *500)* or 5000LOAD.*xxx* (for the *DYNASTAR 100e, 2000,* and *5000),* where *xxx* represents a 3-digit number that identifies the software version.

CAUTION: If you are upgrading a remote unit from pre-6.04 software, you must use a different upgrade procedure from the one given below. Please consult your release notes or contact a *DYNASTAR* representative.

COMPRESSED CONFIGURATION FILE

Upgrading *DYNASTAR* operating system software may reset the existing configuration in the unit. This means that remote access to the unit is lost, since its IP configuration has been lost. The configuration cannot be uploaded or downloaded once remote access is lost, since TFTP does not work without IP access to the unit.

Uploading or downloading a compressed configuration file along with system software retains remote access to the unit. When the ASCII configuration file is transferred, the *DYNASTAR* reads dynamically from and writes to the configuration in the SRAM without actually storing the file into the file system. However, the compressed configuration file transfer feature allows the user to upload the compressed version of the **config** file from the unit and download it back to the unit's file system along with the new version of the operating system. When the *DYNASTAR* is reinitialized, it loads the new operating system, and the compressed configuration file is detected in flash memory and used to retain the previous configuration.

While the binary configuration file described in the section *Binary Upload/Download,* later in this chapter, can only be used for the same version of the operating system, the compressed configuration file can span different versions of the software. However, be aware of potential consequences, such

as duplicating IP addresses, if you plan to use the compressed file uploaded from one unit to configure a different unit.

NOTE: The compressed configuration file feature is supported in software versions from 6.01.1 onward.

To perform a remote upgrade using the compressed configuration file, follow the procedures in the section *Download from an IP Workstation.* For additional information on the *DYNASTAR* configuration file, see the section *Uploading/ Downloading DYNASTAR Configuration Files*.

CAUTION: Be sure to download the correct CNFGLOAD.CMP file to the *DYNASTAR* along with other system modules before restarting the unit, or the current configuration—and possibly access to the unit—will be lost.

VERIFYING CODE VERSIONS

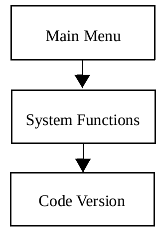
You can verify the version of software installed on your *DYNASTAR* by accessing the Code Version screen.

1. From the Main Menu, select **System Functions**.

✓ The System Commands screen (Figure 4-1) appears.

2. Fom the System Functions screen, select **Code Versions**.

✓ The Directory Management screen shown in Figure 4-14 appears. This screen shows the DOWNLOAD.BIN file that is loaded on your system. You can view the subfiles that make up the DOWNLOAD.BIN fileon the Applications menu (Figure 4-3).




```
                         ***Directory Management***

File Name        Loaded/Created      Size      Version       Expected     Erase
DOWNLOAD.BIN  10-09-02   13:01   1114880     6.08 <RC45>                     N
SRAM1            10-14-02    8:41       13620     6.08 <RC45>                     N
SRAM2            10-14-02    8:23       13510     6.08 <RC45>                     N






                                                     Compress Directory? N


_______[DynaStar 399c]______                  Enter password to erase files: _________
Use TAB & CURSOR keys to move among fields                Press ESC to exit screen
```

Figure 4-14 Directory Management Screen

DOWNLOAD FROM AN IP WORKSTATION

Trivial File Transfer Protocol (TFTP) can be used in an IP environment to:

- Transfer files to/from the *DYNASTAR*
- Erase flash memory
- Restart or reinitialize the *DYNASTAR*

TFTP can be run on any IP host, such as a PC, workstation, or minicomputer. The transmission path from the TFTP device to the *DYNASTAR* can be over a LAN, dedicated synchronous PPP line, X.25, frame relay, or any combination of media.

NOTE: For TFTP file transfers to be performed, IP routing must be enabled on the Ethernet Port Configuration menu (from the Main menu, select **Configuration**, then **Port**, then **Port 0**), unless an alternate path has been provided.

The TFTP examples shown in this section are based on running TFTP on a PC using the PC/TCP package available from FTP Software. If you are using a different package, you might enter the commands in a somewhat different format.

NOTE: If you need to retain the current configuration of the *DYNASTAR*, you must upload the compressed configuration file **cnfgload.cmp** from the *DYNASTAR* and then download it with the other files. For more information, see *Uploading/Downloading DYNASTAR Configuration Files* later in this chapter.

To load new software:

1. Make a working copy of the *DYNASTAR* software diskette.
2. Turn the *DYNASTAR* on. To update the software on the *DYNASTAR*, the unit must be up and running.
3. Make sure that the *DYNASTAR* has access to the server you are transferring files to or from. (This is the IP Address entry for Port 0, accessed from the Router menu.) You may want to PING the *DYNASTAR*'s IP address before transferring files to make certain the connection is OK.
4. If you want to retain the existing *DYNASTAR* configuration, while the *DYNASTAR* is running the old software version, upload the compressed configuration file from the unit in binary mode using TFTP.

   For example, using PC/TCP, enter:

   tftp get cnfgload.cmp <ip_address> cnfgload.cmp image <return>

✓ The *DYNASTAR* creates the compressed configuration file in flash memory and delivers a copy to the IP address specified.

5. Now erase flash memory. Use TFTP to send any ASCII file to the *DYNASTAR*. The destination file name must be a concatenation of “erase” and the Supervisor password.

For example, using PC/TCP, enter:

tftp p u t\junk 197.100.100.15 erase\secret

where junk might be replaced by any filename and 197.100.100.15 is the IP address of the remote *DYNASTAR*.

NOTE: Flash erasure takes at least 90 seconds.

6. Use TFTP to send the download file to the *DYNASTAR*, using binary mode.

NOTE: The download file is called DOWNLOAD.BIN for the *DYNASTAR 100*, *100i*, and *500*. It is called 5000LOAD.BIN for the *DYNASTAR 100e*, *2000*, and *5000*. However, when downloading 5000LOAD.BIN it must be renamed DOWNLOAD.BIN.

For example, using PC/TCP, enter:

tftp put download.bin 197.100.100.15 download.bin image<return>

7. Verify the downloaded file:

- Use TFTP to get *.BIN from the *DYNASTAR*, using binary mode (where * replaces the actual filename).
- Compare the file to the original file.

  For example, using PC/TCP, enter:

  tftp get junk.bin 197.100.100.15 download.bin image<return>

  where 197.100.100.15 is the IP address of the remote *DYNASTAR*.

  comp junk.bin download.bin<return>

CAUTION: Make sure that the file has been successfully loaded to the *DYNASTAR* before reinitializing it. If this is not the case, attempt to download again. If the file cannot be loaded successfully,

the *DYNASTAR* will be isolated if you restart it. Contact your customer service representative for assistance.

8. If you want to retain the current configuration, download the compressed configuration file to the unit along with other system software.
For example, using PC/TCP, enter:

tftp put cnfgload.cmp <ip_address> cnfgload.cmp image <return>

✓ The *DYNASTAR* will retain its configuration when reinitialized.

9. Reinitialize the *DYNASTAR*. Use TFTP to send any ASCII file to the *DYNASTAR*. The destination filename is a concatenation of “reinit” and the Supervisor password. For example, using PC/TCP, enter:

tftp p u t\junk 197.100.100.15 reinit\secret<return>

NOTE: Using the reinit command preserves the previous configuration stored in flash in step 8. If you do not wish to save the previous configuration, you can use “restart” as part of the command string. For example:

tftp pu t\junk 197.100.100.15 restart\secret<return>

DOWNLOAD FROM A *DYNASTAR*

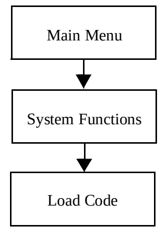
Another method of upgrading *DYNASTAR* system software is to download the software from an operational *DYNASTAR*.

NOTE: The CNFGLOAD.CMP file, used to preserve the current configuration in the *DYNASTAR*, is not transferred when an upload or download is performed from the Download/Upload menu of the *DYNASTAR*.

To update application software, connect to the Supervisor on a *DynaStar* (referred to as the local *DynaStar*).

```
*** Download to or Upload from Remote System ***

Enter IP address of remote system:                      0.0.0.0
(IP host or another DynaStar)

Press <RET> to select type of remote system:            DynaStar

                                                        Continue (Y/N): Y

_________[DynaStar_3df2]__________
                                              Press ESC to return to previous menu.
```

Figure 4-15   Download/Upload Menu



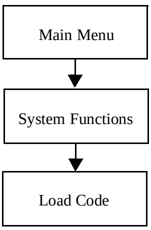
Use the *DynaStar* System Download/Upload menu (Figure 4-15) to:

- Download code from the local *DynaStar* to a remote *DynaStar*
- Download code from the local *DynaStar* to a remote IP host
- Upload code from a remote *DynaStar* or IP host to the local *DynaStar*.

NOTE: The *DynaStar* must be able to establish a connection to the IP address of the remote *DynaStar* or IP host. The IP address must be in the same IP internet as the local *DynaStar*, and at least one serial or LAN link to the remote system must have the IP application enabled.

To download files to the remote device:

1. From the Main menu, select **System Functions**.



✓ The System Commands menu (Figure 4-1) is displayed.

2. Select **Load code**.

✓ The Download/Upload menu (Figure 4-15) is displayed.

3. Enter the IP address of the remote device in the field provided (Figure 4-16).

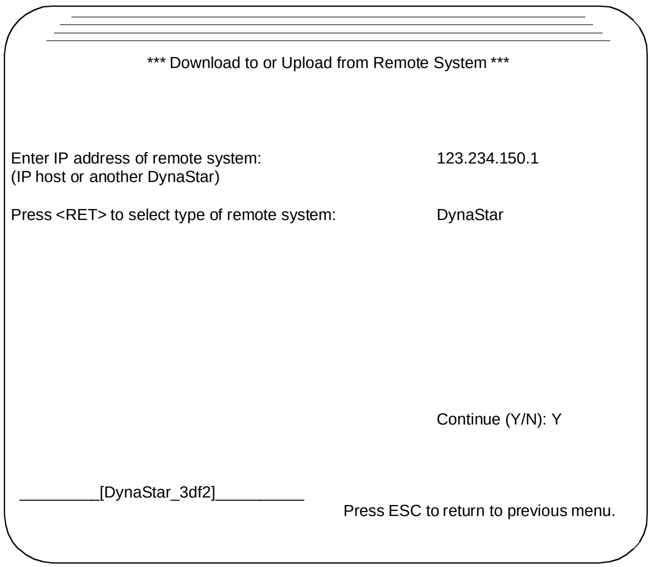


Figure 4-16 Enter IP Address and Select Remote System Type

4. Select the type of remote device (***DynaStar*** or **IP Host**). Use the cursor keys to move to the field and the return key to toggle the values until the desired value is displayed.

5. In the **Continue** field, enter **Y** and press **<return>**.

✓ If a connection is established to another *DynaStar*, you are prompted to enter its password (Figure 4-17).

```
*** Download to or Upload from Remote System ***

Enter IP address of remote system:                123.234.150.1
(IP host or another DynaStar)

Press <RET> to select type of remote system:      DynaStar

Enter password of remote DynaStar:

                                                  Continue (Y/N): Y

_________[DynaStar_3df2]__________
                                         Press ESC to return to previous menu.
```

Figure 4-17 Enter the Remote *DYNASTAR* Password

6. Enter the password.

✓ A message appears telling you to wait for remote system verification (Figure 4-18).

✓ If the verification succeeds, the System File Name screen (Figure 4-19) appears. (If verification fails, you receive an error message.) The Local File Names screen shows the date and time the various files were loaded onto the local *DYNASTAR* and the size of the files (in bytes).

NOTE: If the remote device is an IP host, you can change the file names to match those loaded on the IP host.

```
*** Download to or Upload from Remote System ***

Enter IP address of remote system:                    123.234.150.1
(IP host or another DynaStar)

Press <RET> to select type of remote system:          IP Server

                WAIT for remote system verification

                                                      Continue (Y/N): Y

_________[DynaStar_3df2]__________
                                       Press ESC to return to previous menu.
```

Figure 4-18 Wait for Remote System Verification

```
                    *** Local File Names ***
File Name           Download date          Size
DOWNLOAD.BIN        2-14-02   13:23:34   1017088
ETH8LOAD.BIN        2-14-02   13:24:15     44544
DMAPLOAD.BIN        2-14-02   13:24:20     50176
QUADLOAD.BIN        2-14-02   13:24:26     85248
ETHERNET.BIN        2-14-02   13:24:41     15616
816PLOAD.BIN        2-14-02   13:26:45     26452
T1E1LOAD.BIN        2-14-02   13:26:55     84736
DBRILOAD.BIN        2-14-02   13:28:45     28746
VRTXOSI1.BIN        2-14-02   12:28:52    346624
ATICLOAD.BIN        2-14-02   13:29:15     26433
                    *** Remote File Names ***
Remote name for DOWNLOAD.BIN:      DOWNLOAD.BIN
Remote name for ETH8LOAD.BIN:      ETH8LOAD.BIN
Remote name for DMAPLOAD.BIN:      DMAPLOAD.BIN
Remote name for QUADLOAD.BIN:      QUADLOAD.BIN
Remote name for ETHERNET.BIN:      ETHERNET.BIN
Remote name for 816PLOAD.BIN:      816PLOAD.BIN
Remote name for T1E1LOAD.BIN:      T1E1LOAD.BIN
Remote name for DBRILOAD.BIN:      DBRILOAD.BIN
Remote name for VRTXOSI1.BIN:      VRTXOSI1.BIN
Remote name forATICLOAD.BIN        ATICLOAD.BIN
                                                 Continue (Y/N): Y
_________[DynaStar_3df2]__________
Terminate input with <RET>.          Press ESC to return to previous menu.
```

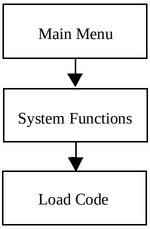
Figure 4-19 File Names Screen for Remote *DYNASTAR*

7. To continue, enter **Y** in the **Continue** field and press **<return>**.

✓ The Download/Upload Commands menu (Figure 4-20) is displayed.

```
              *** Download to or Upload from Remote System ***



      IP address of remote system:      123.234.150.1

      1.   Download files from this DynaStar to remote system
      2.   Upload files from remote system to this DynaStar
      3.   Verify files from remote system to this DynaStar
      4.   Restart remote DynaStar


      Enter command number:






_________[DynaStar_3df2]__________
Terminate input with <RET>.                   Press ESC to return to previous menu.
```

Figure 4-20 Download/Upload Commands Menu



8. Use the **Download files** command to transfer local files to the remote system.

✓ If the remote system is a *DYNASTAR*, remote flash memory is erased before the files are transferred.

9. Use the **Verify files** command to verify that local and remote files are identical.

✓ The *DYNASTAR* uploads the DOWNLOAD.BIN file from the remote system and compares the file to the local file residing in flash memory.

10. Use the **Restart remote *DYNASTAR*** command to restart the remote system.

```
*** Download to or Upload from Remote System ***

IP address of remote system:      123.234.150.1

1.   Download files from this DynaStar 500 to remote system
2.   Upload files from remote system to this DynaStar
3.   Verify files from remote system to this DynaStar
4.   Restart remote DynaStar

Enter command number: 1

Flash erased OK.
DOWNLOAD.BIN transferred OK.
ETH8LOAD.BIN transferred OK.
DMAPLOAD.BIN transferred OK.
QUADLOAD.BIN transferred OK.
ETHERNET.BIN transferred OK.
816PLOAD.BIN transferred OK.
T1E1LOAD.BIN transferred OK.
DBRILOAD.BIN transferred OK.
ATICLOAD.BIN transferred OK.
VRTXOAI1.BIN transferred OK.


_________[DynaStar_3df2]__________
                                  Press ESC to return to previous menu.
```

Figure 4-21 Download Files Command Status Reports

✓ While files are being downloaded or uploaded or the flash memory is being erased, the operation that is being performed is displayed (see the example in Figure 4-21). The success or failure of the operation is displayed when it is completed.

Figure 4-21 shows status reports for the **Download** command. Similar reports are displayed for the other commands.

■ UPLOADING/DOWNLOADING *DYNASTAR* CONFIGURATION FILES

Using TFTP, configuration files can be downloaded to a *DYNASTAR* from an IP workstation or uploaded from a *DYNASTAR* to an IP workstation, independently of the *DYNASTAR* system software.

NOTE: The *DYNASTAR* in either case must have software version 5.01 or higher (and PROM version 3.9 or higher) installed.

CONFIGURATION FILE OPTIONS

Configuration files can be transferred in different ways, depending on your requirements.

ASCII CONFIGURATION FILE (config). This file can be used to configure multiple units with similar network configurations. In other words, the same configuration file is downloaded to different remote units, but certain parameters, such as names and IP addresses must be customized for each unit. This can be achieved by uploading the ASCII configuration file from one unit, manually modifying the file, and downloading it to a different unit. For the download to be accomplished, the unit must be running and accessible via IP. An ASCII **config** file can be downloaded to different units running different software versions. This feature is supported for Versions 5.01 and above. For more information, see the sections that follow.

COMPRESSED ASCII CONFIGURATION FILE (CNFGLOAD.CMP). This is the compressed version of the file described in the previous paragraph. Since it cannot be modified manually, the file cannot be used to configure different units, but it can span different software versions. This is especially useful when *DYNASTAR* software is being upgraded. This feature is supported forVersions 6.03 and above. For more information, see the earlier section in this chapter, *Compressed Configuration File.*

NOTE: While it is not necessary to load this file during a software upgrade, the file allows you to retain access to a remote *DYNASTAR* by preconfiguring it.

STATIC BINARY CONFIGURATION FILE (SRAM). This is a binary image of the current configuration of the unit. It can only be used for a specific unit and a specific software version. Its main purpose is to assist customer support in troubleshooting specific configuration problems. For more information, see the section *Binary Upload/Download* later in this chapter.

ASCII CONFIGURATION FILE FORMAT

The configuration file contains only those parameters contained on menus in the Configuration menu hierarchy. These parameters include port, protocol, and application settings. Configuration file parameters and their values are defined in the *DYNASTAR* MIB. A copy of the MIB is available through your customer service representative.

A configuration file consists of a header and a body. A sample header file is illustrated in Figure 4-22.

HEADER. The header begins and ends with a series of hashes. The purpose of the header is to provide system-specific information to the user. Do not edit header file information.

```
#################################################################
########
#WARNING: Do not edit any information in the header or information followed
#by '%' in the body without the complete understanding of the consequences.
#
#UNIT TYPE: DS100
#DATE: 6/17/96
#DAUGHTER BOARDS: 1) QUAD 2) 16-PORT 3) NODAUGHTER 4) NODAUGH-
TER    5) 16-PORT
% 1 24
% 1 35
% 1 63
% 1 71
% 1 84
#
#
#
############################END HEADER######################
```

Figure 4-22   Sample Header File

BODY. The body consists of the configuration information along with comments to aid you in reading and editing the configuration file. Any line in the body that starts with a hash symbol (#) is taken as a comment and is ignored. The lines beginning with % are control statements that carry important configuration information in the download process. A sample configuration body file is illustrated in Figure 4-23.

```
#                              Port - 0
#
% 20
3.1.2.1      portGen1AdminPortNumber = 6
3.12.3       portGen1AdminProtocol = 13
3.1.2.4      portGen1AdminPortName = Ethernet
#                           LAN Options
%30
3.2.2.1      portLANAdminPortNumber = 0
3.2.2.3      portLANAdminApplicationsBridge = 2
3.2.2.4      portLANAdminApplicationsIPXRouter = 2

#                        IP Router Options
% 17 0
5.2.4.2.1.2  routerAdminIPAddress = 199.97.52.29
5.2.4.2.1.3  routerAdminIPMask = 255.255.255.0
5.2.4.2.1.4  routerAdminIPProtocol = 1
```

Figure 4-23 Sample Configuration Body

TFTP Configuration Parameters. Any line that is not a comment (beginning with #) or a control statement (beginning with %) is a configuration parameter. The configuration parameters are written into the file on a port-by-port basis. These are followed by the application parameters. Each parameter has three fields:

- **ID**: Identifies the configuration parameter and cannot be edited.
- **Name**: Unique object name that corresponds to the ID.
- **Value**: Numerical value of the configuration parameter.

How to Retrieve an ASCII Configuration File

You can retrieve a *DynaStar* configuration file with a TFTP *get* operation. When you retrieve a configuration file from a *DynaStar*, **config** is always the name of the file to be retrieved. If you wish, you can store the file on your workstation or server using a name that will help you identify it later.

How to Load an ASCII Configuration File

You can load a configuration file into a *DynaStar* from a workstation using a TFTP *put* operation. The target filename must be **config**/*password* (where *password* is the supervisor's password on the target *DynaStar*).

Suggestions:

1. Use the Ethernet LAN port (Port 0) to upload or download the configuration file if the IP address of the port you are using to perform the file transfer will change once the file has been downloaded to the *DynaStar*.

2. When downloading a *DynaStar* configuration from one unit to another, make sure that the types of daughterboards installed in the target *DynaStar* match the daughterboards installed in the source *DynaStar* or that there is no daughterboard in the corresponding slot in the target unit.

   NOTE: If the **config** file was retrieved from a unit running Software Version 5.01 or 6.0, name the destination file **config.501**/*password* or **config.60**/*password*, respectively. A destination name of **config**/*password* can be used as explained earlier for Version 6.01 and later versions.

BINARY UPLOAD/DOWNLOAD

Using TFTP, a binary image of a *DYNASTAR* configuration can be downloaded to or uploaded from the SRAM segment of Flash memory. You can use this capability to create an archive of different configurations or to assist customer support in troubleshooting specific configuration problems.

When you perform a binary transfer, files are copied directly to or from Flash memory without affecting the current configuration.

To upload binary files, perform a TFTP *get* command and use one of the following filenames:

SRAM1

SRAM2

SRAM

The filenames with numbers retrieve the contents of SRAM copy #1 or copy #2; the filename SRAM retrieves the contents of the copy of SRAM that is currently active.

To download a binary copy of SRAM:

1. Erase the contents of both SRAM #1 and #2. Use TFTP to put

   ERASE1/*password*

   and then

   ERASE2/*password*

   where *password* represents the administrator's password for the destination *DYNASTAR*. (The default is **secret**.)

2. Write SRAM #1 or #2 using TFTP to put

SRAM1/*password*

or

SRAM2/*password*

NOTE: The binary files should be downloaded only to a *DYNASTAR* with exactly the same software version and the same daughterboard and interface module configuration as the *DYNASTAR* from which the code was originally uploaded.

CAUTION: Do not change a screen configuration while an SRAM upload or download is in progress.

3. Warm start the *DYNASTAR* to make the new configuration take effect.

■ FALLING BACK TO A PREVIOUS VERSION

It is possible to fall back to a previous *DYNASTAR* configuration (if one exists) after your download if you discover problems with the current configuration.

The Directory Management screen (Figure 4-14) shows the currently loaded file versions. The most recent configuration is stored in SRAM1. The previous configuration is stored in SRAM2. You can erase SRAM1 on the Directory Management screen and then perform a warm start of the unit. This will force the unit to begin using the SRAM2 configuration. The warm start menu also allows you to select the operating system version that you want to use.

CONTACT ALARM AND RELAY MODULE

5

■ OVERVIEW

The Contact Alarm and Relay module can be installed in all *DYNASTAR* models. It provides 48 dry contact inputs and 8 controllable relay outputs per module. One contact module can be installed in the *DYNASTAR 100*, two in the *DYNASTAR 100e* and *DYNASTAR 2000*, and a maximum of five contact modules in the *DYNASTAR 500* and *DYNASTAR 5000*. For the latter two units, this extends the number of contacts to 240 inputs and 40 outputs.

The module continuously monitors the inputs and generates TL1 formatted alarm messages or SNMP traps that can be forwarded to centralized management control centers. A typical use of the Contact module is shown in Figure 5-1.

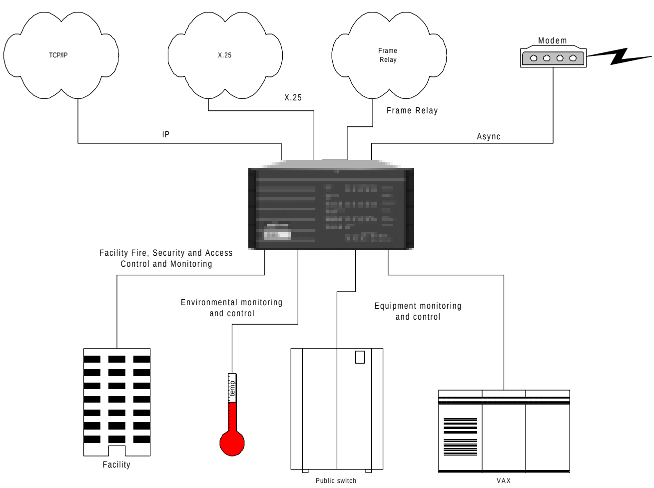


Figure 5-1 Example of Contact Module Use

The LED display for the contact alarm shows green if no contacts are in alarm and red otherwise.

■ APPLICATIONS

TL1 APPLICATION

In the TL1 application, the management system typically opens up a TL1 session to the Contact module virtual port using asynchronous, X.25, IP, or OSI connectivity. Once a TL1 session is established, either all the alarms that are set can be reported, or the user can request the status of a particular alarm or set of alarms. New alarms are reported in real time as long as the management system remains connected. The alarms are generated in accordance with Bellcore TL1 alarm format for equipment and environmental inputs.

The Contact module supports a number of standard TL1 messages, as well as the standard equipment and environmental alarm formats. The following input commands are accepted by the Contact module application: ACT-USER (used to establish a session); CANC-USER (used to break a session); RTRV-HDR (used during a session, usually every 15 minutes, as a “keep alive” indicator); RTRV-HISTORY (used to return the alarm history for the unit); and RTRV-ALM-ALL, RTRV-ALM-EQPT, RTRV-ALM-ENV (used to retireve all/equipment/environment contact inputs that are currently in alarm state).

In addition, there are commands to manipulate the CONTROL outputs. These outputs are dry-contact relays with a Normally Open (NO) and Normally Closed (NC) pair. The command OPR-EXT-CONT activates a relay changeover, which has an optional momentary action. The command RLS-EXT-CONT releases a relay changeover. The momentary action is defined in milliseconds, with 250 mS resolution.

The traces below show the responses expected from these commands. In these examples, the TID name is “dynastar,” the user ID is “root”, the password is “secret”, and the user tag is “dys”. (The user tag [C-TAG] is optional and is used to differentiate among users having the same TID.)

ACT-USER

Format: Command:TID:User_ID:C-TAG::Password;

Input: act-user:dynastar:root:dys::secret;

Response:

```
 DynaStar 99-10-29 18:05:53
M DYS COMPLD
;
```

RTRV-HDR

Format: Command:::C-TAG;

Input: rtrv-hdr:::dys;

Response:

```
  DYNASTAR 99-10-29 18:07:34
M DYS COMPLD
;
```

CANC-USER

Format: Command:TID:User_ID:C-TAG;

Input: canc-user:dynastar:root:dys;

Response:

```
  DYNASTAR 99-10-29 18:08:01
M DYS COMPLD
;
```

RTRV-ALM-ALL

Format: .Command:TID:User_ID:C-TAG;

Input: rtrv-alm-all:dynastar:root:dys;

Response:

```
DYNASTAR 99-10-29 18:08:01
M DYS COMPLD
  “AID1:CR,SA,,,ALARMMSG.”
;
```

RTRV-ALM-EQPT and RTRV-ALM-ENV are similar to RTRV-ALM-ALL above.

OPR-EXT-CONT

Format: Command:TID:AID:CTAG:CONT:,DURA;

Input: opr-ext-cont:dynastar:relay1:dys::;

Response

DYNASTAR 99-10-29 18:08:01
M DYS COMPLD
;

For the command above, the AID is defined in the Contact card menu. The CONT field is not required and can be skipped by entering another ":". The DURA field follows the CONT field and optionally defines a momentary changeover when the contact will activate for a period of time and then reset automatically. The period is in mS (milliseconds) with a granular spacing of 250mS. For example a changeover of 3 seconds would require a DURA of "3000". The DURA field, unlike other commands uses a "," spacing character

Example: Command:TID:AID:CTAG::,3000;

RLS-EXT-CONT

Format: Command:TID:AID:CTAG:CONT,DURA;

Input: rls-ext-cont:dynastar:relay1:dys::;

Response

DYNASTAR 99-10-29 18:08:01
M DYS COMPLD
;

The AID and CONT fields are as described for the previous command. The TL1 messages are configured from the menu-driven message table (Figure 5-4) that lets you quickly format the message content from toggle options. You can also configure the messages manually to support custom options.

SNMP Application

In the SNMP application, the alarms generated from changes in contact inputs are formatted into SNMP traps. These traps can be directed to an SNMP server or to a management system supporting SNMP. The SNMP trap messages can be directed to up to four management systems.

Controlling Relay Outputs from SNMP. An SNMP application can also control relay outputs through multiple SET commands. The MIB identifies three special locations for controlling a relay output.

This is basically a three-step operation.

1. Write the AID into the correct location. MIB Object ID "1.3.6.1.4.1.14797.2.2.3.1.5.16.2.2.1.16" is the location that sets the relay you want to control. It is the AID defined in the contact card setup screen and the relay that AID controls. This string must be sent as an ASCII string and is case sensitive.
2. If momentary operation of the relay is required, then MIB Object ID "1.3.6.1.4.1.14797.2.2.3.1.5.16.2.2.1.17" is the location that sets the timer value for momentary changeover. This value is an integer in milliseconds. For example, 10000 represents 10 seconds.
3. To operate the relay, MIB Object ID "1.3.6.1.4.1.14797.2.2.3.1.5.16.2.2.1.18"is the location that activates the relay. The value "1" releases the relay, "2" activates the relay, and "3" activates the momentary operation set by the timer value in step 2.

Please see Appendix C for additional information about SNMP.

■ CONTACT MODULE CONFIGURATION

Configuration of the Contact module consists of the following four steps:

- Configure the message table
- Define the Contact module's virtual port
- Select TL1 or SNMP
- Configure TL1 or SNMP specific parameters, including security options

CONFIGURE THE MESSAGE TABLE. To configure the message table, follow the procedure below:

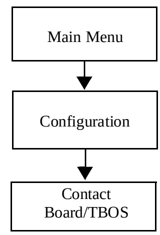
1. From the Main menu, select **Configuration**.
2. From the Configuration menu, select **Contact Board/TBOS**.

✓ The Configure Contact and TBOS Alarms screen appears (Figure 5-2).

3. Select **Add/Change/Verify Contact Alarm Parameters**.

```
*** Configure Contact and TBOS Alarms ***

1 - Add/Change/Verify Contact Alarm Parameters
2 - Configure TBOS Display Parameters

Enter contact number:

_________[DynaStar_3df2]__________
Press ESC to return to previous menu.
```

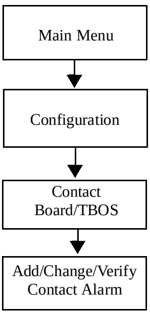
Figure 5-2 Configure Contact and TBOS Alarms Screen



✓ The Contact Table screen (Figure 5-3) appears. If you have not yet defined any alarms, the table will be blank. Otherwise, a list of the configured alarms and their alarm numbers appears. In the *DYNASTAR 500* and *DYNASTAR 5000*, the contact numbers available depend on where the Contact module was installed, as given below:

Slot 1: numbers 1 - 48
Slot 2: numbers 49 - 96
Slot 3: numbers 97 - 144
Slot 4: numbers 145 - 192
Slot 5: numbers 193 - 240

NOTE: Two slots are available for the *DYNASTAR 100e* and *DYNASTAR 2000*.




```
*** Contact Table ***
                                        Last changed: 3-01-02 13:24:33



                        Enter contact number:


_________[DynaStar_3df2]__________
Press ESC to return to previous menu.
To edit/add entry, enter contact # <RET>     Cursor up/down for more entries.
To delete entry, enter contact # <CNTL-D>    NOTE: delete takes place immediately
```

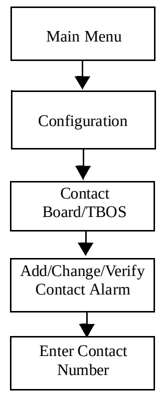
Figure 5-3 Contact Table

4. At the **Enter contact number** prompt, enter the number of the alarm you wish to define.

✓ The Alarms screen (Figure 5-4) appears.

5. Fill in the fields as required. Parameters and values are given in Table 5-1.

6. In the **Process Selections** field, enter **Y** and press **<return>**.




```
*** Alarms ***

| - Press <RET> to toggle values - | | -- Type in values. Max chars shown in <> -- |

Alarm Name:              <8>

Alarm Access Identifier:                        <20>  Contact No: 1

TL1 Type: REPT ALM EQPT                         Alarm Code: CRITICAL

Alarm Type:                                     Locn: NEND

Alarm Cond: DISABLED                            Dirn: RCV

Off Code: SET                                   Serv Aff: SA

Outputs:

Alarm Message                                                  (64)

                                          Process selections (Y/N): Y

 _________[DynaStar_3df2]__________
 Use <CNTL-D> to delete entry.
 Use Tab & Cursor keys to move among fields. Press ESC to abort command & exit.
```

Figure 5-4 Contact Module Alarms Screen

Table 5-1 TL1 Parameters

Parameter	Description	Value
Alarm Name	A brief name for the alarm	8 alphanumeric characters
Alarm Access Identifier	User definable name that defines the alarm type. Also the name used to define relay output control in ACT-EXT-CONT or RLS-EXT-CONT commands	20 alphanumeric characters
Contact No.	The number of the alarm you are defining.	1 -240 as explained above
TL1 Type	Equipment or environment alarm.	REPT ALM EQPT REPT ALM ENV
Alarm Code	The alarm severity.	Critical Major Minor None

Table 5-1 TL1 Parameters (cont.)

Parameter	Description	Value
Alarm Type	A user-defined name (such as "Cooling") that identifies the alarm group.	9 alphanumeric characters
Alarm Cond	The alarm state.	Open Close Disabled
Off Code	Code sent to the management system to indicate that the alarm has ceased.	Set Clear
Outputs	Defines which relay will be activated for AID defined above. Relays 1-40 are valid depending upon the number of cards installed.	N/A
Locn	Location of the alarm: near or far end. Appears only if TL1 Type = Rept Alm Eqpt.	NEND FEND
Dirn	Direction of the alarm failure: receive or transmit. Appears only if TL1 Type = Rept Alm Eqpt.	Rcv Trmt
Serv Aff	Indicates if the alarm is service affecting or not. Appears only if TL1 Type = Rept Alm Eqpt.	SA NSA
Alarm Message	A user-defined string that provides additional alarm information.	64 alphanumeric characters

DEFINE VIRTUAL PORT. You now need to configure the virtual port for the Contact module. This port provides the interface between the *DYNASTAR* and the management system. The virtual port is assigned an address that allows IP, X.25, or asynchronous connectivity to the Contact module.

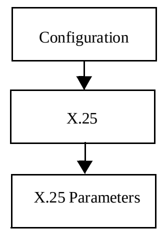
1. If you are at the Contact Module Alarms screen at the end of the previous procedure (Figure 5-4), press **ESC** three times to return to the Configuration menu.

2. From the Configuration menu, select **X.25**.

✓ The X.25 Parameters screen appears (Figure 5-5).

```
                         *** X.25 Parameters***

1  -  Bridge & Router call addresses
2  -  X.121 routing table
3  -  IPX-In & SLIP over X.25
4  -  PVC SVC switching table
5  -  XOT Switching table
6 -  X.121 Address Translation
7  -  Virtual Port Configuration (TIDMUX, CONTACT, OSI)
8  -  TID Definition Table (TIDMUX, CONTACT, OSI)



                        Enter command number:


_______[DynaStar-Dc00375]_______                   Process entries (Y/N):Y
Terminate input with (RET)                   Press ESC to return to previous menu
```

Figure 5-5 X.25 Parameters Screen

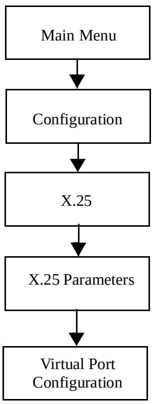


3. Select **Virtual Port Configuration (TIDMUX, CONTACT, OSI)**.

✓ The Virtual Port Configuration Table (OSI, Contact Alarm) appears (Figure 5-6). In the Service column, toggle until **SVC** appears. In the X.25 NUA column, enter the X.121 address of the virtual port. In the APP column, toggle to select **Contact**. (The other fields are not used for the Contact module.)

4. In the **Process Entries** field, enter **Y** and then press **<return>** to save your entries.

✓ You return to the X.25 Parameters screen.




```
     *** Virtual Port Configuration Table (TIDMUX, CONTACT, OSI) ***
                                          Last changed:  5-26-02 9:44:30
  Service          X.25 NUA        APP          LCN #       Port #
  (Toggle)         (SVC only)      (Toggle)          (PVC only)

 1: SVC            123456          CONTACT
 2:
 3:
 4:
 5:
 6:
 7:
 8:
 9:
10:
11:
12:
13:
14:
15:
_______[DynaStar-Dc00375]_______                 Process entries (Y/N):Y
In Service field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.  Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields.Press ESC to abort command & exit.
```

Figure 5-6 Virtual Port Configuration Table

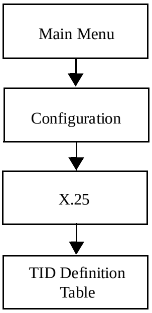
Select TL1 or SNMP and Configure Parameters. In this section of the configuration, you select whether TL1 messages or SNMP traps will be used. For TL1, you must define the TID address used by the host application, as well as login names and passwords. For SNMP, you must define the Host IP address and associated SNMP parameters.

1. If you are at the Virtual Port Configuration Table (at the end of the previous procedure), press **ESC** once to return to the X.25 Parameters screen.
2. Select **TID Definition Table (TIDMUX, CONTACT, OSI)**.

✓ The TID Definition Table appears (Figure 5-7).

```
              *** TID Definition Table (TIDMUX, CONTACT, OSI) ***
                                              Last changed:  5-26-02 9:44:30
   APP              TID               X.121 Address           Port #   TL1/SNMP
   (Toggle)       (22 alphanumeric)    (1-15 BCD)                      (Contact Only)
 1:  CONTACT     DYNASTAR
 2:
 3:
 4:
 5:
 6:
 7:
 8:
 9:
10:
11:
12:
13:
14:
15:

_______[DynaStar-Dc00375]_______                       Process entries (Y/N):Y
In the TID field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.  Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields.Press ESC to abort command & exit.
```

Figure 5-7 TID Definition Table



3. In the APP field, toggle to select **Contact**.

4. In the TID field, enter the TID address for the host application if you are using TL1.

5. In the TL1/SNMP field, toggle to select the mode you will use.

6. In the **Process entries** field, enter **Y** and then press **<return>** to save your configuration.

7. Press **ESC** three times to return to the Main menu.

8. If you selected TL1, continue with step 9 below. If you selected SNMP, skip to step 14.

9. From the Main menu, select **Security**.

✓ The Security menu (Figure 5-8) appears.

Main Menu → Security

```
***Security Commands***

1 -  Password Change      Change Operator Password
2 -  Access Security      Change Operator Access
3 -  IPX-In Security      IPX-In ID strings
4 -  IPX-Out security     IPX-Out service restrictions
5 -  IP Filter            IP Address Filter
6 -  TL1 security         Add/Change TL1 Username/Password
7 -  Network security     Add/Change Network Passwords
8 -  Destinations         Add/Change Permitted Destinations
9 -  Security Options     Validation options and methods
10 - SecurID              Access Authorization
11 - Port Selection       Which ports have security enforced

Enter command number:

_______[DynaStar dc000345]_______
Terminate input with <RET>.          Press ESC to return to previous menu.
```

Figure 5-8 Security Commands Menu

10. From the Security menu, select **TL1 Security**.

✓ The Add/Change TL1 Username/Password screen (Figure 5-9) appears.

11. Enter the new User Name and press **<return>**.

12. At the **Enter New Password** prompt, enter the TL1 password for the selected user name and press **<return>**. Reenter the password at the **Confirm Password** prompt.

13. Repeat steps 9 through 11 as required to configure additional user names and passwords.

✓ For TL1 users, your Contact module configuration is now complete.

14. For SNMP users, select **Configuration** from the Main menu.

```
*** Add/Change TL1 Username/Password ***

        TL1 User Name

 1 -- SuperUser
 2 -- Ops
 3 --
 4 --
 5 --
 6 --
 7 --
 8 --
 9 --
 10 --

_______[DynaStar-Dc00375]_______
To modify username, enter new name <Ret>        To delete entry, enter <CNTL-D>
To change Pwd, cursor to name <CNTL-C>    Press ESC to abort command & exit.
```

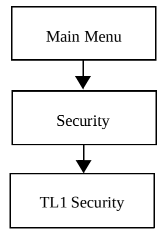


Figure 5-9 Change TL1 Password Screen

15. From the Configuration menu, select **SNMP**.

✓ The SNMP Parameters screen (Figure 5-10) appears.

```
                         *** SNMP Parameters ***
                                   Last changed:  5-26-02 9:44:30

 -------------------------Enter a maximum of 48 characters--------------------
 System description:        DynaStar 100
 System contact:
 System name:
 System location:
 Read-only Community name:
 Read-write Community name:
 Private Community name:

 ----------------Enter 4 integers, 0-255, separated by a period------------
 Trap IP address:   0.0.0.0             Trap IP address:    0.0.0.0
 Trap IP address:   0.0.0.0             Trap Ip address:    0.0.0.0

 ---------------Use RET to toggle value----------------------------
 Enable authentication: N
 Enable traps:          N
 GUI Display Type (for DynaStar 100/100i): RACK MOUNT
_______[DynaStar-Dc00375]_______                    Process selections (Y/N):Y
To change or add entry, enter new value.  Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields.Press ESC to abort command & exit.
```

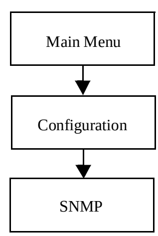


Figure 5-10 SNMP Parameters Screen

16. Set **Enable Traps** to **Y**.

17. Enter the IP address(es) of the management system(s) where traps will be sent.

18. Enter other information as desired.

19. At the **Process selections** prompt, enter **Y** and press **<return>** to save your configuration.

✓ For SNMP users, your Contact board configuration is now complete.

■ PHYSICAL CONNECTIONS

The Contact module uses two RJ-45 (8-pin) connectors to connect to the remote contacts and relay controls. Eight pairs of connectors (identified as A through H) are available on the Contact I/O module (see the top portion of Figure 5-11). The pinout of the connectors is given in Table 5-2. Recommended methods for terminating the Contact I/O connectors are shown in Figure 5-11 and Figure 5-12.

Table 5-2 Contact Module Pinouts

Connector J1

Pin #	Pin Name	Description
1	C2 RTN	Contact C2 Return
2	C2 IN	Contact C2 Input
3	C3 RTN	Contact C3 Return
4	C1 IN	Contact C1 Input
5	C1 RTN	Contact C1 Return
6	C3 IN	Contact C3 Input
7	C4 RTN	Contact C4 Return
8	C4 IN	Contact C4 Input

Table 5-2 Contact Module Pinouts (cont.)

Connector J2

Pin #	Pin Name	Description
1	C6 RTN	Contact C6 Return
2	C6 IN	Contact C6 Input
3	Relay Output N.O. A	Isolated relay contact R1. Normally open contact (N.O.) when power to the *DYNASTAR* is off
4	C5 RTN	Contact C5 Return
5	C5 IN	Contact C5 Input
6	Relay Output A Return	R1 Return
7	Relay Output N.C. B	Isolated relay contact R1. Normally closed contact (N.C.) when power to the *DYNASTAR* is off.
8	Relay Output B Return	R1 Return

Figure 5-11 illustrates a termination method where each I/O board RJ-45 module connector is connected to a special converter head (Hubbel #BR-866JC). This special connector head lets you use an RJ-45 flat cable between the *DYNASTAR* and a standard 66 punch-down block. The Hubble connector is designed to fit directly over a span of 8 punch down contacts. Each I/O pair of connectors from a *DYNASTAR* requires 16 punch-down contacts.

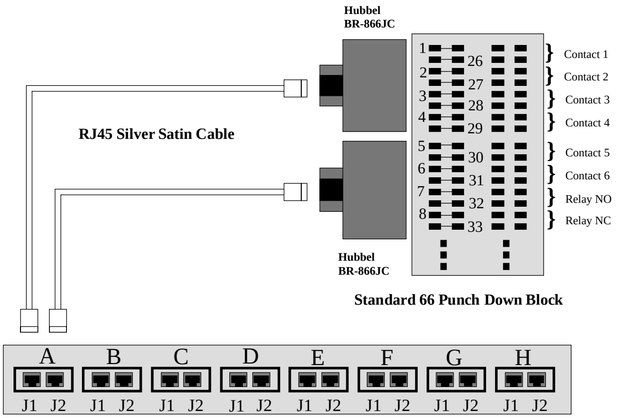


Figure 5-11 Contact Module Connection to Converter Head

Figure 5-12 illustrates a second method for terminating the *DYNASTAR* Contact module. This method uses a special header (Hubble # BR-2580 BF) that converts six RJ-45 flat ribbon cables onto a Telco 50-way connector used by many phone systems. These 50-way connectors are also available on standard 66 punch-down blocks. Use this method if the preferred wiring between the *DYNASTAR* and a punch-down block is the Telco 50-way cable. The special header can be used to locally terminate the RJ-45 connectors on the rear of the Telco cable.

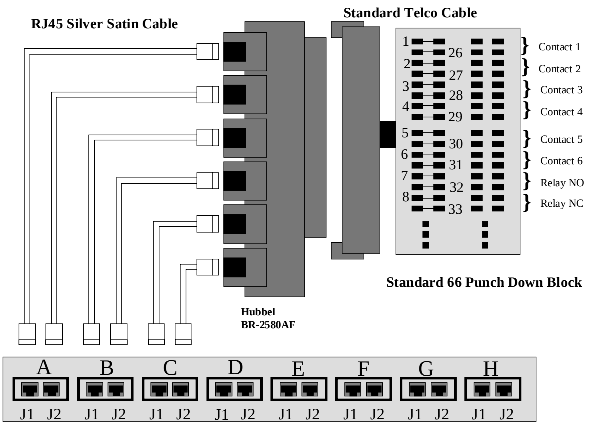


Figure 5-12 Contact Module Connected to Telco Connector

Exact connections used when the Contact module is installed in different slots of the *DYNASTAR 500* or *DYNASTAR 5000* are given in Appendix E, along with technical specifications.

The X.25 Application

Introduction

The *DynaStar* integrates several traditional X.25 functions into a single system. A port configured for X.25 traffic can support traditional X.25 connections as well as remote LAN connections and X.25 traffic over IP and TCP/IP networks:

- The *DynaStar* can be used as an X.25 concentrator and can route packets over a standard X.25 network. The *DynaStar* supports standard X.121 addressing and address translation on both incoming and outgoing connections.
- The IPX-Out application can operate over X.25 networks, giving LAN workstations access to services provided by public and private PDNs.
- IPX-In and SLIP can be used over X.25 to connect asynchronous devices to a Novell LAN.
- Multi-protocol routed and bridged traffic can be carried on the same X.25 access link. Each virtual call provides a link to a different distant server and can be configured to support IP routing, IPX routing, or Ethernet bridging.
- X.25-In and X.25-Out can be used to allow an X.25 user to reach a TCP/IP device or a TCP/IP device to reach a remote X.25 device.
- The *DynaStar* provides a Telnet gateway over X.25. This is described in detail in Chapter 13, *Telnet and Async Services*.
- XOT allows X.25 traffic to be encapsulated in TCP/IP traffic and routed over an IP backbone network.

This chapter explains how to configure the X.25 port and also describes the configuration of bridge and router traffic over X.25, the X.25 concentrator function, and XOT.

Other functions that use X.25 are described elsewhere. IPX-In, IPX-Out, and SLIP are discussed in Chapter 12,

6

The X.25 Application

The IP/IPX Router Application. X.25 over ISDN is explained in Chapter 9, *ISDN Configuration*, and SNA over X.25 is explained in Chapter 14, *SNA over X.25 and Frame Relay*. X25In and X25Out are described in Chapter 13, *Telnet and Async Services*.

X.25 is also often used in conjunction with asynchronous devices such as PADs. See Chapter 7, *The PAD Function*, for details about the PAD function and support for call mnemonics and Network User IDs (NUIs).

■ X.25 PORT CONFIGURATION

To use X.25 to connect to a PDN or to use it as the underlying protocol for LAN access, you must first configure at least one of the WAN ports in your *DYNASTAR* to support X.25.

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) appears.

2. Select **Port**.

✓ A list of available ports, similar to the screen in Figure 6-1, appears.

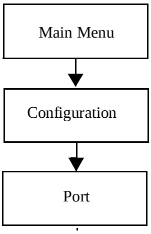
3. Select the port that you want to configure with the X.25 protocol and enter that port's number at the **Enter port number** prompt.

✓ A menu showing the port parameters that are currently set for the port appears.

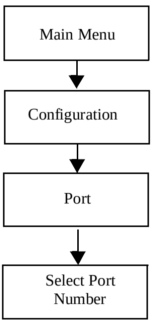
NOTE: You must select a port that is capable of handling the X.25 protocol. These ports are the baseboard ports labeled HS WAN and Sync/Async, any QUAD port, any port on the 8-port or 16-port sync/async board, any BRI or PRI B-channel, or any D-channel on which X.25 has been enabled.

```
*** Configure Port ***

Valid port numbers (with names) are:
 0: Ethernet
 1: HS 8-port card
 2: 16-port card
 4: ATM slot 4
 5: Dual T1/E1
 6: Console
 7: Sync/Async
 8: HS WAN 1
 9: HS WAN 2
10: Virtual PAD
99: Virtual X.25 Ports

                          Enter port number:

_________[DynaStar_3df2]__________
Terminate input with <RET>.              Press ESC to return to previous menu.
```

Figure 6-1 Typical Configure Port Screen



4. If the port is not currently configured as X.25, toggle the **Port type** field until **X.25 line** appears and press **<tab>**.



✓ The screen displays the parameters that need to be configured for X.25, as shown in Figure 6-2.

```
                              ***X.25 Port Configuration***
 Port: 5  IS-35                                          Last changed:  5-23-02  11:26:45

|- Press <RET> to toggle values. -|  |-Type in values. Max chars shown in () --|
Port type:             X.25 line           Port name:   HS WAN 1                    (14)
                                            X.121 Address:                       (15 BCD)
Connection mode:              DTE
Line speed:                9.6 kbps         Non-Zero DTE Cause:    N
Number of flags:(0-15)          0           Allow User Data:       Y
Calling address mod:         NONE           LAPB extended:         N
Local Address insert:           N           X.25 mode:             DTE
Max Window size:                7           K LAPB window size:    7                (fixed)
Max Packet size:             1024           T1 Acknowledgment timer:3          (1-255 sec)
Packet/Window Neg:              Y           T3 Idle Timer:         30          (0-255 sec)
Require CUG:                    N           N2 Retransmission count:20             (1-255)
Require NUI:                    N           N1 Max frame size:     8248 bits
Req Reverse Charging:           N            LCN Partition    Base LCN      Number of VCs
Route inbound calls on CUD:     N                             (1-4095)
Traffic types permitted on line                Permanent:       1                0
      IP Routing:                Y             One-way in:      1                0
      IPX Routing:               Y             Two-way:         1                4095
      Ethernet Bridging:         Y             One-way out:     4095             0


 _______[DynaStar_3614]_______                      Process selections (Y/N): Y
 Use TAB & CURSOR keys to move among fields.   Press ESC to abort command & exit.
```

Figure 6-2 X.25 Port Parameters Screen

5. In the **Port name** field, give the port a name that will help you identify this port. This name will appear in any list of the ports, such as the list from which you select a port to configure.

6. In the **X.121 Address** field, enter the X.121 address of this port. If the port has been assigned an address by the PDN, enter that address here. See the section *X.121 Addressing* later in this chapter for more details on addressing in X.25 networks.

7. In the **Connection mode** field, select **DTE**, **DCE**, or **Dial**.

✓ If you select **Dial**, the **Line speed** field is changed to **Modem speed** and a new line is added for the modem command.

8. Fill in the rest of the values as required by your network. See Table 6-1 for an explanation of all parameters and possible values.

NOTE: If this port will be supporting IP routing, IPX routing, or Ethernet bridging, be sure to set the appropriate value(s) to **Y** under **Traffic types permitted on line**. Otherwise, set the values to **N**.

9. When your configuration is complete, enter **Y** in the **Process selections** field and press **<return>**.

10. If you have configured the line as a dial line, complete your configuration by configuring the X.121 routing, as explained in the section *The X.25 Concentrator* later in this chapter.

Table 6-1 X.25 Port Parameter Values

Parameter	Description	Values
Port type	The type of traffic the port will handle. **<return>** toggles through permissible values. A menu specific to the type selected appears when the cursor is moved from the field.	X.25 line PPP Frame relay, etc. Default=PPP
Port name	A name to help you identify this port.	Max 14 chars
X.121 Address	The address used to call this port. See *X.121 Addressing* later in this chapter for more information.	Max 15 BCD digits Default=null
Connection mode	The physical level connection of the port. *DCE* means that the port is a physical DCE that provides clocking. *DTE* means that the port is a physical DTE device looking for an external clock source. *Dial* provides dial-on-demand services to users who do not require a dedicated circuit, as well as dial backup for failed X.25 links. **NOTE**: Be sure that one end of your connection provides physical DTE and that the other end provides physical DCE.	DTE=default DCE Dial

Table 6-1 X.25 Port Parameter Values (cont.)

Parameter	Description	Values
Line speed	Line speed depends on the electrical interface and connection mode as given below: V.24 direct & leased: 1.2-64kbps V.24 dial: 2.4-64kbps V.35/X.21 dir & lsd: 9.6-2048kbps V.35/X.21 dial: 9.6-128 kbps	1.2 kbps - 2.048 Mbps Default depends on line configuration
Number of flags	Provides the “throttle” feature that is used to insert additional flags between frames. This is often used for older equipment that requires more than a single flag between frames.	0-15 0=default
Calling address modification	Specifies how the calling address in incoming call packets is handled. If the value is *Insert* and the received incoming call packet does not have a calling address, the port’s X.121 address is inserted. If the value is *Replace*, the X.121 address is inserted in all incoming call packets. If the value is *Unique*, all calls (up to 16 per port) will have a unique calling address that substitutes a value from 00 to 15 for the last two digits of the port calling address.	None=default Insert Replace Unique
Local Address insertion	When enabled, inserts the X.121 address of the alternate X.25 port as the calling address when the call could not be established over the highest priority line, but was sent instead over an alternate route.	Y N=default
Max Window size	The packet level window size. For X.25 and bridge and router calls, the size specified for this parameter is used.	2-7 7=default
Max Packet size	The maximum packet size. For X.25 and bridge and router calls, the size specified for this parameter is used.	128, 256, 512, 1024 1024=default

Table 6-1 X.25 Port Parameter Values (cont.)

Parameter	Description	Values
Packet/ Window Negotiation	Allows you to enable or disable window and packet negotiation at the packet level on a port-by-port basis.	Y=default N
Require CUG	Specifies whether the X.25 network requires Closed User Groups to be used.	Y N=default
Require NUI	Specifies whether the X.25 network requires Network User Identification to be used.	Y N=default
Require Reverse Charging	Specifies whether reverse charging is required on outgoing calls.	Y N=default
Route inbound calls on CUD	Allows a call to be routed using the data contained in the Call User Data field of the incoming X.25 call packet rather than routing the call on the called address. This is intended for calls destined for PAD ports.	Y N=default
Traffic types permitted on line	Indicates whether IP, IPX, and/or Ethernet bridged traffic are allowed on this X.25 line.	Y=default N
Modem Command	Hayes AT command set sent to modem upon initialization (displayed only in Dial mode)	User defined
Non-Zero DTE Cause	If set toY, clear and reset causes may have a value other than zero. Applies to the DTE only.	Y N=default
Allow User Data	Specifies whether Call Request packets are allowed to contain a 16-byte Call User Data field.	Y=default N
LAPB extended	LAPB extended numbering (modulo 128) supports extended sequence numbers for efficient operation across media that have long delays, such as satellite links.	Y N=default
X.25 mode	Operation of the link at the logical level.	DTE=default DCE

Table 6-1 X.25 Port Parameter Values (cont.)

Parameter	Description	Values
K LAPB window size	The link level window size. Fixed at 7 if LAPB extended=N.	7-127 7=default
T1 Acknowl-edgment timer	The LAPB retransmission timer.	1-255 seconds 3=default
T3 Idle Timer	The LAPB idle timer.	0-255 seconds 30=default
N2 Retrans-mission count	The link level retransmission counter.	1-255 20=default
N1 Maxi-mum frame size	Based on the value of LAPB extended.	8248 8256
LCN Partition	An internal LCN map for defining the LCN address space for X.25 PVCs, and one-way incoming, two-way, and one-way outgoing SVCs. For each type of LCN, the selectable values specify the beginning LCN number (base LCN) and the maxi-mum number of virtual circuits that can use that type of LCN. Ranges for the different types of LCNs cannot overlap. A validity check on LCN ranges and numbers is made when **Y** is entered in the **Process selections** field. **NOTE**: Your LCN range must match the LCN range of the remote equipment	1-4096 (LCNs) 0-256 (VCs)

■ BRIDGE AND ROUTER CONFIGURATION OVERVIEW

The *DYNASTAR* can establish a virtual call over an X.25 link to any distant bridge or router that can be reached through the X.25 Public Data Network (PDN). The distant bridge or router can be connected directly to the PDN or can be connected through PDN managed gateways. Requirements for the distant bridge or router, based on the application traffic carried on the link, are summarized in Table 6-2.

Table 6-2 Bridge and Router Requirements

Application	Distant Device	Protocol Compliance
IPX Router	*DYNASTAR* Access Server	RFC 1362
IP Router	Any IP Router	RFC 1356
Ethernet Bridge	Any Ethernet Bridge	IEEE 802.1d, RFC 1356

You configure the bridge and router function by entering the called X.121 address of the remote device in the bridge and router address table. A maximum of 60 X.121 addresses can be entered. However, if 60 X.121 addresses are specified and all three applications (IP, IPX, Bridged) are permitted for each entry, it is possible to have 180 simultaneous virtual calls.

The *DYNASTAR* automatically tries to establish a virtual call for Ethernet bridge traffic and IPX router traffic to each X.121 address where the application is permitted. If the call attempt is unsuccessful or if an established virtual call is cleared, the *DYNASTAR* tries to reestablish the call at the frequency defined by the X.25 call setup retry timer. For IP router traffic, the *DYNASTAR* sets up calls when there is traffic to send. The unit tries to establish a virtual call to each X.121 address where the application is permitted and where the IP addresses match.

WARNING: If IP router is set to N, TFTP and SNMP traffic cannot be exchanged with the distant IP router unless there is an alternate path.

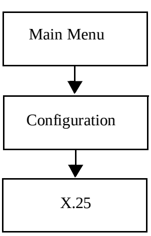
CONFIGURING BRIDGES AND ROUTERS

The following procedure explains how to configure your X.25 ports to handle bridge and router traffic.

NOTE: Before you begin this procedure, you must have already configured the X.25 ports that you will use (see *X.25 Port Configuration* earlier in this chapter).

1. From the Main menu, select **Configuration**.
2. The Configuration Commands menu appears (Figure 3-11).
3. Select **X.25**.

✓ The X.25 Parameters menu, shown in Figure 6-3, appears.




```
***X.25 Parameters***

1 - Bridge & Router call addresses
2 - X.121 routing table
3 - IPX-In & SLIP over X.25
4 - PVC/SVC switching table
5 - XOT switching table
6 - X.121 Address Translation
7 - Virtual Port Configuration (TIDMUX, CONTACT, OSI)
8 - TID Definition Table (TIDMUX, CONTACT, OSI)

Enter command number:

_______[DynaStar  dc000345]_______
Terminate input with <RET>.                    Press ESC to return to previous menu.
```

Figure 6-3 X.25 Parameters Menu

4. From the X.25 Parameters menu, select **Bridge & Router call addresses**.

✓ The X.121 Addresses for Bridge and Router Calls menu, as shown in Figure 6-4, appears.

5. In the **Distant X.121 address** field, enter the X.121 address of the port on the distant end where the X.25 bridge or router call will terminate.

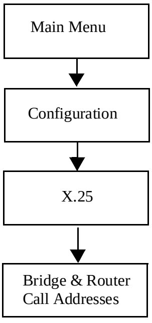
6. In the **Port** field, toggle to enter the X.25 port on which the virtual call should be established.

7. In the **Traffic** field, indicate whether bridged, IPX, and/or IP traffic will be supported for this X.121 called address.

   NOTE: If all traffic types are enabled, IP and IPX packets will be routed, and all other protocols will be bridged. To bridge IP and/or IPX traffic, enter an N in the IP/IPX fields.

```
                 *** X.121 Addresses for Bridge and Router Calls***
                                               Last changed: 5-26-02  7:00:45

  Distant X.121 address    |--Use RET to toggle values--|    Distant IP Address
    (1-15 BCD)             Port #      Traffic:  B   IPX   IP             x.x.x.x

 1:
 2:
 3:
 4:
 5:
 6:
 7:
 8:
 9:
 10:
 11:
 12:
 13:
 14:
 15:

_______[DynaStar 35dd]_______                        Process X.121 selections (Y/N):
In X.121 address field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.   Use <CTRL-D> to deleteentry.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 6-4 X.121 Addresses for Bridge and Router Calls Menu



8. If IP traffic is permitted, enter the distant IP address in the **Distant IP Address** field. This IP address must be part of the same IP network as the X.25 line.

   NOTE: Be sure that only valid destinations are listed in this column.

9. When you have completed all your entries, enter **Y** in the **Process X.121 selections** field and press **<return>**.

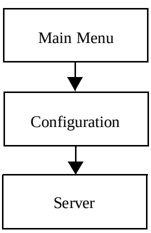
✓ You are at the X.25 Parameters menu.

10. Press **<ESC>**.

✓ You are at the Configuration menu.

11. Select **Server** from the Configuration menu.

✓ The Systemwide Parameters screen, as shown in Figure 6-5, appears.




```
                         *** Systemwide Parameters***

Server name: DynaStar399c                                              (47)
Supervisor console herald:      DynaStar Supervisor                    (32)
Dial IP idle timer:             2      (0-disable, 1-254 min, 255-10 sec)
Dial IPX idle timer:            2                  (0-disable, 1-255 min)
Dial Bridge idle timer:         2                  (0-disable, 1-255 min)
B Channel call timeout:         0                 (0-disable, 1-1440 min)
X.25 call set-up timer:         5                              (1-30 min)
XOT Idle Timer                  0                   (0-disable, 1-30 min)
PPP IP prioritization:          0                     (0 - disable, 1-99)
IPX-In preferred File Server:                                          (47)
IPX-Out broadcast address:      399c                                    (8)
Reserved LCNs:                  N                           <CR> to toggle
Exhaustive Routing:             ENDPOINT                    <CR> to toggle
x32 No LCN Drop Timer:          6               <0-disable, 1-12<10 sec>>
Daughter Board Auto-Recover:    Y                           <CR> to toggle


_______[DynaStar 399c]_______                 Process selections (Y/N): Y
Use <TAB> and CURSOR to move fields.   Press ESC to return to previous menu
```

Figure 6-5 Systemwide Parameters Screen

12. Set the **X.25 call setup retry timer** to the value you want. (The default value is 5 minutes.) This value indicates how often the *DynaStar* will try to set up calls that have cleared or that could not initially be established.

13. When you have set the timer, enter **Y** in the **Process selections** field and press **<return>**.

14. If you enabled the IP Routing function in the Bridge and Router screen (step 7), you must complete the configuration of your IP routes in the IP Addresses menu and the IP Static Routes menu. See Chapter 12, *The IP/IPX Router Application*, for more information.

■ THE X.25 CONCENTRATOR

The X.25 concentrator function routes incoming calls from an X.25 or PAD port to outbound X.25 lines. The routing algorithm consults the X.25 Concentrator Routing table whenever an incoming call does not terminate in the *DYNASTAR* at a PAD port, the supervisory process, or a LAN application.

X.121 ADDRESSING

Destinations in an X.25 network are designated by an address, which contains from 1 to 15 digits. For example, in the network illustrated in Figure 6-6, A's address is 12345 and B's address is 67890. If A were to place a call to B, the *called* (destination) address would be 67890 and the *calling* (source) address would be 12345.

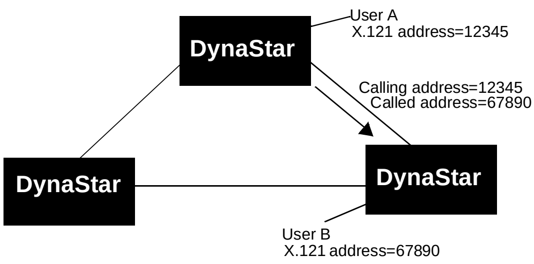


Figure 6-6 Private Network Showing X.121 Addressing

The address scheme shown in Figure 6-6 is a simple one similar to those often used on private X.25 networks. If the *DYNASTAR* were connected to a public data network (PDN), the *DYNASTAR* port would be assigned an address by the PDN so that it would be reachable by other users of the PDN. PDN addresses tend to be longer than private addresses. For

example, in the United States, PDN addresses normally consist of 14 digits.

The routing function in the *DYNASTAR* is based on called X.121 addresses. To provide maximum flexibility during configuration and to reduce the number of entries in the routing table, the *DYNASTAR* lets you enter the letters D and X in the routing table in addition to the digits 0 through 9. A “D” is a placeholder for any single digit. For example, a table entry of 1DD would be a match for 123, 144, 167, 193, and so on. An “X” stands for any number of digits or for no digits. There can be only one X per address, and the X must be placed either at the beginning or the end of the address. For example, X23 is a match for all of the following: 23, 123, 4455623, and so on.

SHARED ROUTING

You can configure two or more paths to the same destination to be *shared routes*. When paths are configured as shared, the routing algorithm balances the traffic over the designated routes by calculating the number of LCNs used on each route and placing a new call on the route that has the fewest number of currently active LCNs. This is also called load balancing. You configure shared entries in the X.25 routing table after you have configured the routes.

CONFIGURATION OF ROUTES

NOTE: The X.25 port must already be configured before you can configure the concentrator function (see *X.25 Port Configuration* earlier in this chapter).

1. From the Main menu, select **Configuration.**

✓ The Configuration Commands menu appears.

2. Select **X.25**.

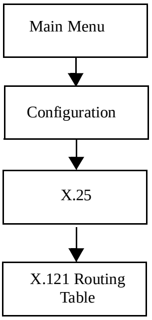
✓ The X.25 Parameters menu (Figure 6-3) appears.

3. Select **X.121 routing table**.

✓ The X.25 Concentrator Routing table, as shown in Figure 6-7, appears.

```
                    ***X.25 Concentrator Routing Table***
                                            Last changed: 4-23-02  7:00:45

  X.121 address    Shared   |--Use RET to Toggle--|          X.32 dial line phone #
 (1-15 BCD D&X) Scheme    Port      Priority    Dial speed       (max 19 characters)
1:
2:
3:
4:
5:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:
_______[DynaStar 35dd]_______                    Process Routing tables (Y/N):  Y
Search for X.121 Address:                        Select Share Scheme:
To change or add entry, enter new value.         Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 6-7 X.25 Routing Table Menu



4. In the **X.121 address** field, enter the *called* address that is to be routed out an X.25 port.

   NOTE: Up to 255 X.121 addresses can be entered, but with the use of D's and X's, a single entered address can represent multiple called addresses.

5. In the **Port** field, toggle to enter the number of the X.25 port to which the call will be routed.

6. In the **Priority** field, enter the priority for this destination, from 0 to 3, with 0 being the highest priority. If it is possible to route the call on more than one port, the *DYNASTAR* will first attempt to route the call on the port having the highest priority. If this fails, it will attempt to route the call using the port that has the next highest priority.

7. In the **X.32 dial line phone #** field, enter up to 19 characters of a modem AT or V.25bis command. (Precede the characters with AT for a modem call, or CRN for a V.25bis call.)

   NOTE: If the X.25 port is configured with a dial modem, the unit uses the modem command to make a telephone connection for an X.32 call to the PDN. Once the X.32 link is connected, multiple virtual calls can be established. The X.32 link is disconnected when all virtual calls are cleared.

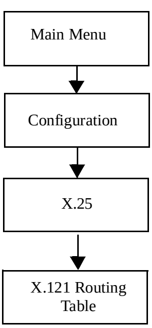
8. Enter **Y** in the **Process Routing Tables** field and press **<return>** to save your configuration and quit.

✓ To aid in finding route numbers, the routing table is automatically sorted by digit and port number.

CONFIGURATION OF SHARED ROUTES

To configure shared routing:

NOTE: The routes that you want to designate as shared routes must already be configured in the X.25 Concentrator Routing Table before you start the following procedure.



1. Reaccess the X.25 Concentrator Routing table (Figure 6-7) by selecting **X.121 Routing Table** from the X.25 Commands screen.

2. In the **Search for X.121 address** field at the bottom of the menu, enter the destination address of the routes that you want to define as shared routes.

3. In the **Select Share Scheme** field, toggle to enter **SHARE**. (The available choices are **SHARE**, **TEST**, and **NONE**.)

   NOTE: If **TEST** is entered, a screen appears showing all routes matching the address in the order that they will be matched. For this to work, any addresses entered must have been saved.

NOTE: If you want to remove shared status from an existing shared route, select **NONE** in the **Select Share Scheme** field and process the selection.

4. Enter **Y** in the **Process Routing Tables** field and press **<return>**.

✓ This saves your entry and returns you to the X.25 Routing table. If you access the X.25 routing table again, you will see the indication **SHARE** in the **Share Scheme** column of the appropriate addresses.

NOTE: Each address that you want to designate as shared must be configured and saved individually.

ROUTING ALGORITHM

Because of its multifunctionality, the *DYNASTAR* can potentially make several checks of the called address before it decides how to route a given call. The flowchart in Figure 6-8 shows the order in which the checks are made. If none of the checks produces a match with the called address, the call is cleared. PVC/SVC and XOT are explained later in this chapter. Async services are explained in Chapter 13, *Telnet and Async Services;* OSI is explained in Chapter 16, *OSI.Gate*.

When searching for a route for a call, the *DYNASTAR* implements what is called exhaustive routing. The *DYNASTAR* initially sends the call via the best route for the particular destination. If the destination is unavailable via that route (line down, congestion, etc.), the *DYNASTAR* consults the routing function again to see if there is an alternate path. The *DYNASTAR* continues to try all possible paths until one reaches the destination or until all paths have been tried unsuccessfully. In the latter case, the call is then cleared back to the source.

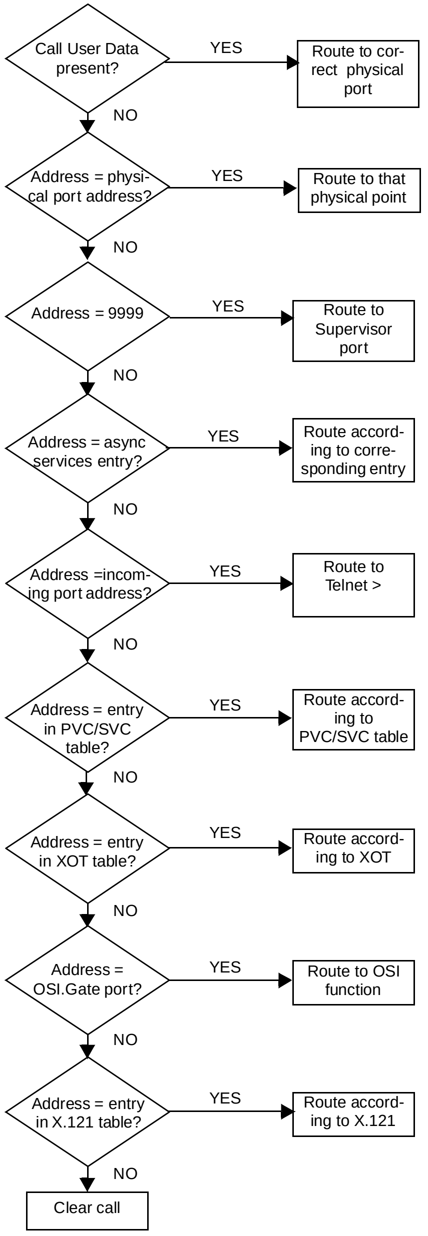


Figure 6-8 X.25 Routing Algorithm Flowchart

■ ADDRESS TRANSLATION

In some routing situations for X.25 calls, it is necessary to convert a called or calling X.121 address into a different address. This conversion is called *address translation*. For example, in the network illustrated in Figure 6-9, the two *DYNASTAR*s are connected through a PDN. Normally, the addressing scheme used on the private units (the *DYNASTARS*) is simpler than the addressing scheme used on the PDN, which, in the United States, generally requires a 14-digit address. Because of this, it is necessary to translate the private address into a public address as the call exits the *DYNASTAR* and then to translate the public address back to a private address as the call reaches its destination on the remote *DYNASTAR*.

As another example, address translation would be needed if two private networks that use different addressing schemes are connected together.

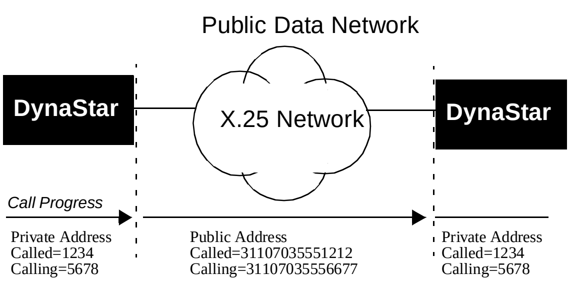


Figure 6-9 Example of Using Address Translation

The *DYNASTAR* address translation feature provides a flexible method for handling all address translation needs for both inbound and outbound called and calling addresses. Inbound address translation occurs as the call enters the *DYNASTAR* before it is routed to its destination. Outbound address translation occurs after the call is routed but before it exits the *DYNASTAR*.

ADDRESS MATCHING. The inbound and outbound addresses are compared to addresses that you have entered in the X.121 address translation table. Entries in the table can

contain the digits 0 through 9, the letter D, or the letter X. As explained in the section *X.121 Addressing,* the letter D represents any single digit, while the letter X represents any number of digits or no digit at all.

Table 6-3 provides examples of using these notations and shows the resulting translations. The **Called or Calling Address** is the address as contained in the Call Request packet. The **From** address is the original address as given in the translation table, and the **To** address is the resulting address as given in the translation table. The **Resulting Translation** is the actual address that will be placed in the Call Request packet after the translation function completes its processing based on the address given in the **Called or Calling Address** column.

Address translation supports the use of nulls to provide an address for a null calling address or to insert a null address when one has initially been provided. The last entry in Table 6-3 illustrates this.

Table 6-3 Address Translation Examples

Called or Calling Address	"From" Address	"To" Address	Resulting Translation
12345	12345	67890	67890
12345	123DD	456DD	45645
12345	12X	3X	3345
12345	X5	3110	3110
null	null	333	333

Where possible, the table also provides translations in the reverse direction. For example, take the first entry in Table 6-3. If the address 12345 is presented, it is converted into the address 67890. Conversely, if the address 67890 is presented, it will be translated into the address 12345, and you do not need to explicitly configure this second translation as long as the first one is configured. However, some entries (such as X5--->3110) do not lend themselves to reverse translation.

It is also possible to have the calling address translated based on the value of the called address, and the called address translated based on the value of the calling address. For example, if a called address ("From" address in Table 6-3) of 8001 arrives, the calling address is translated into 5678 (the "To" address). This is indicated in the configuration screen as "Called tr calling." (The reverse would be "Calling tr called.")

Figure 6-10 shows the translation process in the DYNASTAR, using the translation table given in Table 6-4.

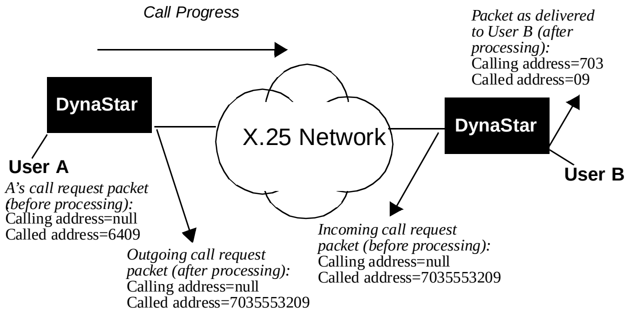
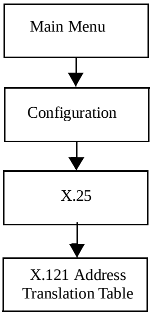


Figure 6-10 Example Address Translation Process

Table 6-4 Address Translation Table for Figure 6-10

	Called/Calling	From	To
User A's Table	Called	64X	70355532X
User B's Table	Called	70355532X	X
	Calling	Null	703

CONFIGURATION. Configure the translations in the X.121 Address Translation table (Figure 6-11), which is accessed from the X.25 Parameters menu. A maximum of 200 entries can be configured.




```
                    ***X.121 Address Translation Table***
                                          Last changed:  5-29-02  16:37:17

     From                To                Port       In/Out      Called/Calling
     (X121, D or X)      (X121, D or X)    (Toggle)   (Toggle)       (Toggle)
 1:  1234567890123       1234567890111       4          In          Called
 2:  703X                301X                4          In          Calling
 3:  3110DDDD01          3110DDDD02          5          Out         Called
 4:
 5:
 6:
 7:
 8:
 9:
10:
11:
12:
13:
14:
15:
______[DynaStar_cd00386]________  Test Entries (CR):   Process Entries (Y/N):
In X.121 address field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value. Use <CTRL-D> to deleteentry.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 6-11 X.121 Address Translation Table

To configure a translation entry:

1. In the **From** column, enter the address that the translation function will compare the inbound or outbound call address to.

2. In the **To** column, enter the address that will replace the inbound or outbound call address.

3. In the **Port** column, toggle to indicate the port to which this translation applies.

   NOTE: If the translation applies to more than one port, you will have to make an additional entry on another line.

4. In the **In/Out** column, toggle to indicate whether this translation applies to inbound calls or outbound calls.

5. In the **Called/Calling** column, toggle to indicate whether this translation applies to the Called address, Calling address, Called tr calling, or Calling tr called.

6. When you have configured all your entries, enter **Y** in the **Process Entries** field and press **<return>**.

   NOTE: If you want to test your entries, see the section *Testing Your Entries* that follows.

Once you have entered and saved your configurations, they will be sorted in the following order:

- Ascending port order
- Inbound/Called followed by Inbound/Calling
- Outbound/Called followed by Outbound/Calling
- Ascending From address
- Ascending To address

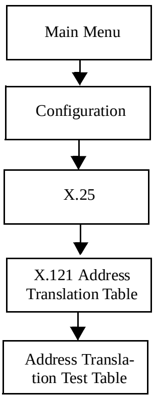
If you reconfigure a port so that it is no longer an X.25 port, the corresponding address translation entries for that port are deleted.

TRANSLATION METHOD. Addresses in inbound and outbound calls are compared to entries in the table to determine if address translation should take place. For incoming calls, addresses are compared before they are routed to their destination. For outgoing calls, addresses are compared after the routing function has determined the call's destination but before it has been sent there.

NOTE: Addresses are also compared on incoming and outgoing extended accepts. These packets include X.121 addresses for both DTE and DCE connections.

If the call address on the designated port matches the **From** address in the table, the call address is replaced with the **To** address. D's and X's are treated as shown in Table 6-3.

TESTING YOUR ENTRIES. Once you have entered your addresses in the X.121 Address Translation table, you can test your entries. You can test to see if a particular address matches the address in the table, and you can see what the resulting address will be. You can test any entry that has been saved in the translation table.



To test an entry:

1. Move the cursor to the **Test Entries** field on the X.121 Address Translation table and press **<return>**.

✓ The Address Translation Test table, as shown in Figure 6-12, appears.

```
                    ***X.121 Address Translation Test Table ***


   Address        Port In/Out      Called/Calling       Matched With    Result
   (X121)             |--------CR to toggle--------|       (X.121)        (X.121)










                                                   Calculate [from ---> to] (CR):
                                                   Calculate [to ---> from] (CR):
________[DynaStar_cd00386]________                 Another Entry (Y/N): Y
In X.121 address field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.   Use <CTRL-D> to deleteentry.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 6-12   Address Translation Test Table

2. In the **Address** field, enter the address that you want to test.

3. In the **Port** field, toggle until the port number that you want appears.

4. In the **In/Out** and **Called/Calling** fields, toggle until the correct indication appears.

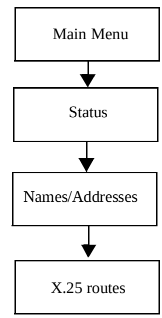
5. Go to the **Calculate [from -> to]** or **Calculate [to -> from]** field, as required, and press **<return>**.

✓ The translation algorithm processes the address you have entered based on the currently saved translation table. If a match is found for the entered address, the matching address from the translation table is shown in the **Matched With** field, and the resulting address

is given in the **Result** field. If there is no match, **Not Found** appears in the **Matched With** column.

6. If you want to test another entry, enter **Y** in the **Another entry** field. If you want to exit the table, enter **N**.

There are also some additional tables that you can use to view information about your X.25 routes. The X.25 Concentrator Routing Table (Figure 6-13) lists all configured X.121 addresses, indicates if they are shared, the port they use, their priority level, and dial speed X.32 phone number, if applicable..



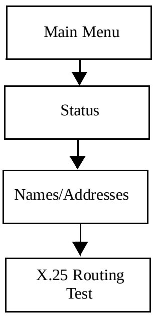
***X.25 Concentrator Routing Table ***

X.121 Address	Shared	Port	Priority	Dial Speed	X.32 Phone Number
123		3	0		
1233		101	0		
543DDD		102	0		

_______[DynaStar_cd00386]________
Use XOFF <CTRL-S> and XON <CTRL-Q>
to control scroll.   Press ESC to return to previous menu

Figure 6-13 X.25 Concentrator Routing Table

The X.25 Test Routing Table (Figure 6-14) allows you to enter an X.121 address at the prompt and receive a list of all matches for that address. This list includes PAD ports, SVC/PVC, OSI, and XOT configurations, and X.121 matches.




```
***X.25 Test Routing Table ***
                                        Results for Address:

Type        Shared Port     Priority/LCN    IP Address      Socket



_______[DynaStar_cd00386]_________
Search for X.121 Address:          Press ESC to abort command & exit
```

Figure 6-14 X.25 Test Routing Table

■ SUPPORT FOR X.25 PVCS AND SVC/PVC SWITCHING

The *DYNASTAR* supports the use of X.25 PVCs (Permanent Virtual Circuits) and switching of X.25 calls from SVCs (Switched Virtual Circuits) to PVCs and from PVCs to SVCs. These types of calls are configured from the X.25 PVC SVC Switching table, accessed from the X.25 Parameters menu.

You define a PVC by assigning a logical channel number (LCN) to a port. For a PVC/PVC call, there will be both an inbound and an outbound assignment. SVCs are represented by an X.121 address that is not associated permanently with any particular port. Each PVC must be unique, but a single X.121 address can be switched to different PVCs.

Once a PVC/PVC call or a PVC/SVC call is configured, the *DYNASTAR* automatically tries to establish the connection. In

the case of a PVC/PVC call, the unit searches the PVC table for a match to the inbound PVC. If a match is found, the call is routed to the corresponding outgoing port using the port and LCN numbers provided in the table. For PVC/SVC calls, the PVC/SVC table is first searched to find an X.121 address corresponding to the given PVC. The asynchronous port and X.121 routing tables are then searched for this SVC called address. If a match is found, the SVC is set up and connected to the PVC.

For SVC/PVC calls, the SVC-to-PVC switching table is searched for the called or calling address (as configured) when an X.25 call request packet is received. If a match is found, the call is answered and connected to the PVC, which is reset. If a match is not found, the call is delivered to the standard X.121 routing routine (SVC/SVC calls).

Configuration of SVC/PVC Switching

The configuration will vary, depending on what type of connection you are configuring. During the configuration, you will not be able to move the cursor to another line until the current line is valid. (You will hear a beep if the line is invalid.) Up to 240 entries (total of all types) can be configured for your *DynaStar*.

NOTE: Before you start this configuration, you must have already configured the X.25 ports that you will use.

PVC/PVC. To configure PVC/PVC calls:

1. From the Main menu, select **Configuration**.

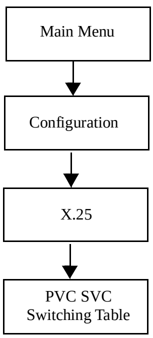
✓ The Configuration Commands menu appears.

2. Select **X.25**.

✓ The X.25 Parameters menu (Figure 6-3) appears.

NOTE: You cannot access this menu unless at least one port has been configured as an X.25 port.

3. Select **PVC/SVC switching table**.



✓ The X.25 PVC SVC Switching table, as shown in Figure 6-15, appears.

```
                         ***X.25 PVC SVC Switching Table***
                                          Last changed:  5-19-02  23:44:01

 SW_Type                    In Bound                        Out Bound
 (Toggle) Port# LCN#  X.121 Address                       Port#   LCN#   X.121 Address
1:
2:
3:
4:
5:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:

________[DynaStar 54ef] ________                   Process entries (Y/N): Y
In SW_Type field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.    Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields.  Press ESC to abort command & exit.
```

Figure 6-15   X.25 PVC SVC Switching Table

4. Toggle the Switching Type (**SW_Type**) field until **PVC/PVC** appears.

5. Configure the incoming side of the PVC by selecting a port number and LCN number under the **InBound** heading.

   NOTE: You can select a port number by toggling through the available X.25 ports. The available LCN numbers are based on the starting LCN number and the number of PVCs allowed for the port as configured in the **LCN Partition-Permanent** section of the corresponding port configuration screen.

6. Configure the outgoing side of the PVC by selecting a port number and LCN number under the **OutBound** heading.

7. To save your entry, enter **Y** in the **Process entries** field and press **<return>**.

SVC/PVC AND PVC/SVC. The configuration of the SVC-to-PVC and PVC-to-SVC connections is identical except that the inbound and outbound sides are reversed. The example below illustrates the configuration of an SVC/PVC connection.

NOTE: For a PVC-to-SVC connection, the called address must be configured in the X.121 routing table or in a PAD port configuration for the call to be routed to its destination.

1. From the Main menu, select **Configuration.**
2. The Configuration Commands menu appears.
3. Select **X.25**.

✓ The X.25 Parameters screen (Figure 6-3) appears.

NOTE: You cannot access this menu unless at least one port has been configured as an X.25 port.

4. Select **PVC/SVC switching table**.

✓ The X.25 PVC SVC Switching table, as shown in Figure 6-15, appears.

5. In the **SW_Type** column, toggle until **SVC/PVC** appears.
6. Enter the SVC address under **X.121 Address** in the **InBound** column. This is the X.25 called address.
7. Enter the port number and LCN number of the PVC in the appropriate columns of the **OutBound** section.
8. To save your entry, enter **Y** in the **Process entries** field and press **<return>**.

■ CONNECTING X.25 EQUIPMENT OVER AN IP-BASED BACKBONE

Remote X.25-based equipment can connect to X.25 host systems over an IP-based backbone, as shown in Figure 6-16. The *DYNASTAR* implements XOT for such connections. This standard, developed by Cisco, encapsulates X.25 packet information within the TCP packets.

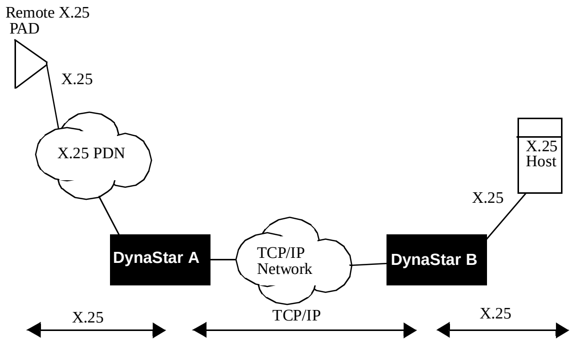


Figure 6-16 Using XOT to Connect X.25 Equipment over a TCP/IP Backbone

XOT provides transparent support for carrying X.25 packets over a TCP/IP network. However, although TCP provides a reliable byte stream for encapsulating X.25 packet information, XOT is needed to ensure that TCP byte streams do not interfere with X.25 packet boundaries. A 4-byte message header is prefixed to the X.25 packet layer information before encapsulation. This header provides a message byte count so that if TCP fragments the packet during transport, the original message can be recovered.

CONFIGURATION. Before you can configure the XOT specific information, you must have already configured an X.25 port to support the application. This port must be able to support the appropriate number of PVCs and SVCs (configured in the **LCN Partition** field of the X.25 Port Configuration screen). See the section *X.25 Port Configuration* earlier in this chapter for information on configuring the X.25 port.

To initiate an XOT transport over a TCP/IP network:

1. From the Main Menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) appears.

2. Select **X.25**.

✓ The X.25 Parameters menu, shown in Figure 6-3, is displayed.

3. Select **XOT switching table**.

✓ The XOT PVC SVC Switching table (Figure 6-17) is displayed. **SVC/XOT** is the default selection.

4. For an **SVC/XOT** entry, tab to the **SVC X121 Address** column and enter the called X.121 address.

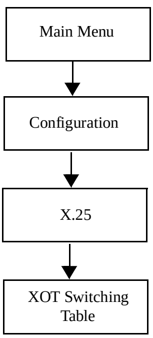
5. For a PVC/XOT entry, press **<return>** to toggle the selection to **PVC/XOT**. Tab to the **Port#** column. Enter the local port number and LCN. Tab again to enter the remote port number and LCN.

6. For both **PVC/XOT** and **SVC/XOT**, tab to the **IP Address** column and enter the remote IP address.

7. To add another entry, press **<return>**.

NOTE: For SVCs, XOT needs to be configured only on the *DYNASTAR* that originates the X.25 calls. For PVCs, configure a corresponding XOT PVC on the remote *DYNASTAR* that will receive the call.

NOTE: The *DYNASTAR* will not let you add another line until all required parameters are completed on the current line.




```
                    *** XOT PVC SVC Switching Table ***
                                          Last changed:  5-14-02  9:44:30
   Service              Local                           Remote
   (Toggle)  Port #    LCN#     X121 Address       Port #   LCN#    IP Address
 1: SVC/XOT                     343556                              123.23.44.1
 2: PVC/XOT    1        33                           6        34    123.23.46.2
 3:
 4:
 5:
 6:
 7:
 8:
 9:
10:
11:
12:
13:
14:
15:
_______[DynaStar-Dc00375]_______                      Process entries (Y/N):Y
In Service field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.  Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 6-17   XOT Switching Table

8. When you have completed your configuration, enter **Y** in the **Process entries** field and press **<return>**.

■ HDLC CONNECTIONS OVER TCP/IP

HDLC over TCP/IP provides end-to-end tunneling of HDLC frames such as frame relay or X.25 data over an IP connection, as shown in Figure 6-18. The *DYNASTAR* implements HDLC over TCP/IP as specified in RFC 1613 (XOT) for such connections. This standard encapsulates X.25 packet information within the TCP packets.

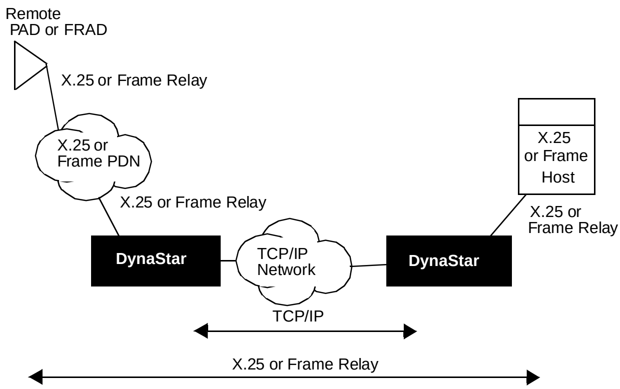


Figure 6-18   HDLC over a TCP/IP Backbone

HDLC over TCP/IP provides transparent support for carrying HDLC frames over a TCP/IP network. However, although TCP provides a reliable byte stream for encapsulating HDLC frame information, encapsulation methods defined in RFC 1613 are needed to ensure that TCP byte streams do not interfere with frame boundaries. A 4-byte message header is prefixed to the HDLC frame information before encapsulation. This header provides a message byte count so that if TCP fragments the frame during transport, the original message can be recovered.

While HDLC over TCP/IP is based on the same standard as XOT, the connection behaves as a PVC and uses LCN 0 over the IP backbone.

CONFIGURING AN HDLC CONNECTION

CONFIGURE THE PORT. First, configure an HDLC port with appropriate parameters:

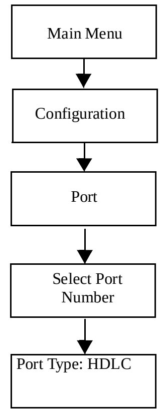
1. From the Main menu, select **Configuration**.
2. From the Configuration Commands menu that appears (Figure 3-11), select **Port**.
3. On the Configure Port menu that appears, enter the number of the port you want to configure and press **<return>**.
4. On the Port Configuration menu, select **HDLC** as the Port Type and tab to the next field.

✓ The menu displays HDLC parameters. Default settings are shown in Figure 6-19.

5. Select the appropriate connection mode and line speed, and indicate the number of flags to be inserted between transmitted HDLC frames.

   NOTE: For more information on these parameters, see the appropriate entries in Table 6-1, *X.25 Port Parameter Values* earlier in this chapter.

6. When you have completed your entries, tab to the Process selections field, enter **Y**, and press **<return>**.




```
                    ***Transparent HDLC Port Configuration***
 Port: 8  IS-232                                   Last changed:  5-1-02  11:26:45
|- Press <RET> to toggle values. -|  |-Type in values. Max chars shown in () --|
Port type:           HDLC                 Port name:    HS WAN1                  (14)

Connection mode:              DTE
Line speed:                   9.6 kbps
Number of flags: (0-15)       0









 _______[DynaStar_3614]_______                    Process selections (Y/N): Y
  UseTAB & CURSOR keys to move among fields.   Press ESC to abort command & exit.
```

Figure 6-19   HDLC Port Parameters Screen.

CONFIGURE THE SWITCHING TABLE. To set up an HDLC connection over a TCP/IP network:

1. From the Main Menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) appears.

2. Select **X.25**.

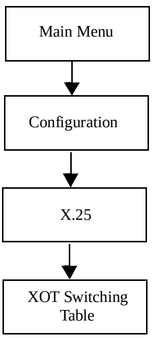
✓ The X.25 Parameters menu (Figure 6-3) is displayed.

3. Select **XOT switching table**.

✓ The XOT PVC SVC Switching table (Figure 6-20) is displayed. This table handles both X.25 over TCP/IP and HDLC over TCP/IP connections. **SVC/XOT** is the default Service selection.

4. Press **<return>** to toggle the Service selection to **HDLC/XOT**.

5. Tab to the Local **Port#** column, and enter the number of the HDLC port for this *DYNASTAR*.



6. Tab to the **Remote Port#** column. Enter the number of the port on the remote *DYNASTAR*.

7. Tab to the **IP Address** column and enter the IP address of the remote *DYNASTAR*.

8. To add another entry, press **<return>**.

   NOTE: The *DYNASTAR* will not let you add another line until all required parameters are completed on the current line.

```
                    *** XOT PVC SVC Switching Table ***
                                         Last changed:  5/16/98  9:44:30
  Service               Local                          Remote
  (Toggle)  Port #    LCN#      X121 Address     Port #    LCN#     IP Address
1: SVC/XOT                      343556                               123.23.44.1
2: PVC/XOT    1         33                          6         34     123.23.46.2
3:HDLC/XOT    3                                     0                123.23.48.2
4:
5:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:
_______[NetPerformer_Dc00375]_______                    Process entries (Y/N):Y
In Service field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value. Use <CTRL-D> to deleteentry.
Use TAB & CURSOR keys to move among fields.Press ESC to abort command & exit.
```

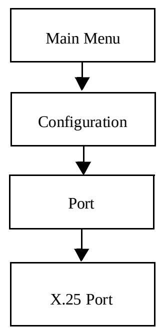
Figure 6-20 XOT Switching Table

9. When you have completed your configuration, enter **Y** in the **Process entries** field and press **<return>**.

■ X.25 IP COMPRESSION

On X.25 ports that are carrying IP traffic, compression can be enabled on a port-by-port basis, rather than a connection basis, meaning that all calls over a given port are compressed if compression is enabled. Currently, only IP traffic can be compressed. Two types of compression are supported: LZS link compression and proprietary link compression. Normally, you will select LZS compression. Select proprietary compression only if the remote end is a *DYNASTAR* that does not support LZS. The average compression ratio over all types of traffic is 1:2.

NOTE: You must enable both ends of a link to support compression. If one end is configured to support compression and the other end is not, the link setup will fail.




```
                         ***X.25 Port Configuration***
Port: 5  IS-35                                    Last changed:  1/1/99  11:26:45

|- Press <RET> to toggle values. -|  |-Type in values. Max chars shown in () --|
Port type:              X.25 line         Port name:    HS WAN                   (14)
                                          X.121 Address:                     (15 BCD)
Connection mode:               DTE
Line speed:               56.0 kbps       Non-Zero DTE Cause:    Y
Number of flags:(0-15)           0        Allow User Data:       Y
Calling address mod:          NONE        LAPB extended:         N
Local Address insert:            N        X.25 mode:             DTE
Max Window size:                 7        K LAPB window size:    7            (fixed)
Max Packet size:              1024        T1 Acknowledgment timer:3       (1-255 sec)
Packet/Window Neg:               N        T3 Idle Timer:         30       (0-255 sec)
Require CUG:                     N        N2 Retransmission count:20          (1-255)
Require NUI:                     N        N1 Max frame size:     8248 bits
Req Reverse Charging:            N         LCN Partition    Base LCN      Number of VCs
Route inbound calls on CUD:      N                          (1-4095)      (2048 total)
Traffic types permitted on line              Permanent:       1              0
    IP Routing:           Y-Compressed       One-way in:      1              0
    IPX Routing:          N                  Two-way:         1              16
    Ethernet Bridging:    N                  One-way out:     17             0


_______[DynaStar_3614]_______                Process selections (Y/N): Y
 Use TAB & CURSOR keys to move among fields.   Press ESC to abort command & exit.
```

Figure 6-21 X.25 Port Parameters Screen with Compression Selected

To enable your *DYNASTAR* to support compression:

1. On the X.25 Port Configuration screen (Figure 6-21), select **Y-Compressed** as the value for **IP Routing**.

2. Enter **Y** in the **Process selections** field and press **<return>**.

3. When your selections are made, press **<ESC>** to exit the menu.

■ The Target Identifier (TID) Multiplexer

You can configure the *DynaStar* as a TID Multiplexer by associating an X.121 address with the TID-Mux application. The TID-Mux multiplexes TL1 messages from a TL1 manager to as many as 60 Network Elements (NEs). This multiplexing function can be used independently or in conjunction with the OSI.GATE switching option that is described in Chapter 16.

Figure 6-22 shows a typical TID multiplexing scenario. A TL1 manager places a call via an X.25 line attached to the *DynaStar*. The *DynaStar* checks the X.121 address in the incoming call request against entries in the Virtual Port Configuration Table (Figure 6-23) and designates the call as a TID Multiplexer call. Once the call is connected, the *DynaStar* extracts Target Identifiers (TIDs) from the data packets received from the TL1 manager and compares them to the entries in the TID Definition Table (Figure 6-24). Valid entries are routed to the specified port.

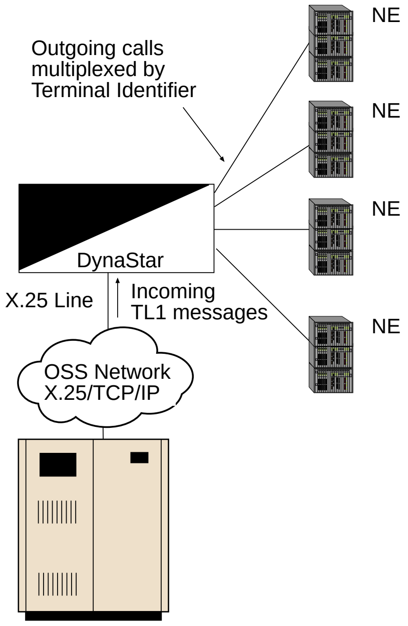
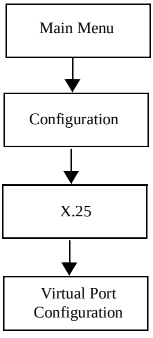


Figure 6-22 TID Multiplexing Example




```
*** Virtual Port Configuration (TIDMUX, CONTACT, OSI) ***
                                       Last changed:  5-16-02 9:44:30
 Service            X.25 NUA          APP           LCN #        Port #
 (Toggle)           (SVC only)        (Toggle)            (PVC only)

 1:  SVC        13579753              TIDMUX
 2:  PVC        12468642              TL1               0            600
 3:
 4:
 5:
 6:
 7:
 8:
 9:
10:
11:
12:
13:
14:
15:
_______[DynaStar-Dc00375]_______                 Process entries (Y/N):Y
In Service field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.  Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields.Press ESC to abort command & exit.
```

Figure 6-23 Virtual Port Configuration Table

Configuring the TID-Mux

To configure an existing X.25 line for TID-Mux use, create a Switched Virtual Circuit (SVC) and then establish routes to NEs as described in the following sections.

Creating a TID-Mux SVC. To set up a TID-Mux SVC:

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. Select **X.25**.

✓ The X.25 Commands menu is displayed.

3. Select **Virtual Port Configuration**.

✓ The Virtual Port Configuration screen (Figure 6-23) is displayed.

4. In the Service field, toggle to select **SVC**.

5. Enter the X.121 address for the SVC in the X.25 NUA field.
6. Toggle the entry in the APP field to **TIDMUX**.
7. Save your entries by entering **Y<return>** in the Process entries field.

ESTABLISHING TID ROUTES. To associate X.121 addresses with the TIDs:

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu is displayed.

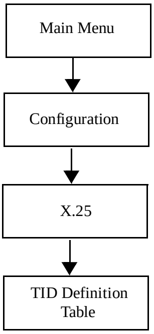
2. Select **X.25**.

✓ The X.25 Parameters menu is displayed.

3. Select **TID DefinitionTable** .

✓ The TID DefinitionTable (Figure 6-24) is displayed.

4. In the APP field, select **TIDMUX**. (No other OSI entries will be available in this field if the OSI.GATE option is not activated in the *DYNASTAR*.)
5. In the TID field, enter a Target ID that may be received in data packets from the TL1 manager.
6. No entry is required in the X.121 Address field.
7. Enter the Port number over which the data for the NE should be routed.
8. When your entries are complete, save them by entering **Y <return>** in the Process entries field.




```
            *** TID Definition Table (TIDMUX, CONTACT, OSI) ***
                                      Last changed:  6-1-02 9:44:30
APP            TID               X.121 Address   Port #      TL1/SNMP
 (toggle)      (22 Alphanumeric) (1-15 BCD)                 <Contact Only>
  1:TIDMUX       BELLTID1        104
  2:OSI-X25      FUNITSU1        73737373
  3:
  4:
  5:
  6:
  7:
  8:
  9:
 10:
 11:
 12:
 13:
 14:
 15:
_______[DynaStar_00375]_______                 Process entries (Y/N):Y
In the TID field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.  Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields.Press ESC to abort command & exit.
```

Figure 6-24 TID Definition Table

THE PAD FUNCTION

7

■ INTRODUCTION

When configured as a PAD, the *DYNASTAR* can provide remote concentration and access for users wanting to connect to public or private data networks. In particular, the *DYNASTAR* provides the following PAD features:

- The *DYNASTAR* allows asynchronous terminals or IP or IPX workstations to connect to an X.25 network.
- Asynchronous terminals connected to an X.25 PAD can reach the *DYNASTAR* Telnet server application.
- The *DYNASTAR* PAD is fully compliant with ITU-T Recommendations X.3, X.28, and X.29.
- Multiple X.3 profiles can be stored in the unit to automate port configuration. Standard ITU-T and user programmable profiles are both supported.
- Network User IDs (NUI) can be configured for increased security.
- Call mnemonics are available for ease of use.
- Sixty-four virtual PAD ports are available for applications such as X25-In and X25-Out (discussed in Chapter 14, *Telnet and Async Services*) and for connecting to remote hosts via X.25 or Telnet.
- Kanji characters can be transmitted and received.
- Ports equipped with the V.90 internal modem WAN interface can be configured asPAD ports for dial in/out access.

■ CONFIGURATION

PAD ports are configured from thePAD Port Configuration screen. This screen is similar to the port configuration screens used for the other protocols. In addition to the port configuration, there are also some systemwide parameters that you need to set forPAD functions.

To configure systemwide PAD parameters:

1. From the Main menu, select **Configuration**.

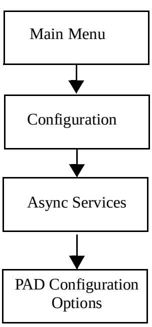
✓ The Configuration Commands menu (Figure 3-11) appears.

2. Select **Async Services**.

✓ The Access Server Commands menu (Figure 3-23) appears.

3. Select **PAD configuration options**.

✓ The PAD Parameters menu, shown in Figure 7-1, appears.




```
                         ***DynaStar PAD Parameters***
                                          Last changed  4-23-02  17:00:34


PAD herald:PAD Port  \P\N\R    (64)

Command mode timeout:          6       (0=disabled, 1-255 ten second increments)

Dial call timeout:             9       (0=disabled, 1-255 ten second increments)

ETB Terminated:                N                                  (CR) to toggle

M-BIT Enable:                  Y                                  (CR) to toggle

PAD Service Signal:                                              (36 chars max)

PAD Service Signal Timer:      0                           (0-disable, 1-60 sec)

_______[DynaStar _399c]_______                Process selections (Y/N): Y
Use TAB & CURSOR keys to move among entries. Press ESC to abort command & exit.
```

Figure 7-1 PAD Parameters Menu

4. Modify the parameter values as required by your network. The parameters are explained in Table 7-1.

5. When your entries are complete, enter **Y** in the **Process selections** field and press **<return>**.

Table 7-1 Description of PAD Systemwide Parameters

Parameter	**Description**
PAD herald	The message that is displayed (along with the physical port number) when you dial in to a PAD port or when you connect a terminal directly. The herald can be up to 64 characters long. The following control characters can be included: \N (line feed), \R (carriage return), and \P (port number).
Command mode timeout	Specifies the amount of time, in 10-second increments, that the PAD can be in command mode without receiving a valid command. If the timer expires before a valid command is entered, the PAD outputs an ERR service signal and returns the terminal to data transfer mode.
Dial call time-out	Specifies the amount of time, in 10-second increments, after which the PAD will free a dial port if no call has been established. The timer is started when the user makes a telephone connection to a dial port. If the timer expires before data is sent, the PAD drops the physical telephone connection.
ETB Terminated	Allows you to configure PAD messages to end with the ETB character required by some networks.
M-BIT Enable	Allows the M-bit to be disabled in outgoing X.25 data packets. When the M-bit is disabled, no X.25 data packets leaving the *DYNASTAR* will have the M-bit set, regardless of the number of bytes in the data packet. By default, the M-bit is enabled. This value can be overridden for individual ports in the port configuration screen.

Table 7-1 Description of PAD Systemwide Parameters (cont.)

Parameter	Description
PAD Service Signal	Prompt that will appear in front of the standard ITU-T asterisk. As part of the prompt, the following can be used: \N (line feed), \R (carriage return), \P (*DynaStar* port number). NOTE: The user-defined service signal works in conjunction with X.3 parameter 6. If, for example, you set the parameter value to 1, the asterisk will not be displayed.
PAD Service Signal Timer	The frequency with which the PAD Service Signal will be resent. Accepted values are 0 (disabled) and 1 to 60 seconds. Default is 0. When the Service Signal Timer is disabled, the user-defined prompt does not appear, although the standard asterisk prompt may appear.

To configure port parameters:

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) appears.

2. Select **Port**.

✓ A list of available ports appears.

3. In the **Enter port number** field, enter the number of the port you want to configure with the PAD protocol.

NOTE: You must select a port that is capable of handling the PAD protocol. This is any asynchronous port on the baseboard or an expansion board.

✓ A screen showing the port parameters that are currently set for the port appears.

4. If the port is not currently configured for the PAD protocol, toggle the **Port type** field until **PAD** appears and press **<tab>**.

✓ The screen displays the parameters that need to be configured for a PAD port, as shown in Figure 7-2.

```
                          ***PAD Port Configuration***
Port 3   IS-232                                  Last changed:  5-29-02  17:00:44

 |---  Press <RET> to toggle values  --| |--- Type in values.  Max chars shown in ()  ---|
Port type:       PAD                 Port name:       sync/async                    (14)

Connection mode:          DCE            Port X.121 address:                  (15 BCD)
Modem speed:              9600 baud      X.121 sub-address:                    (2 BCD)
Parity:                   EVEN           Use sub-address in calling DTE address: N
DSS flow control:         N              Inactivity timer: 0     (0, 1-30 min, 31-255 out)
Call address field:       NONE
NUI Required:             N              Enter ? <RET> for profile list
Mnemonic Type:            NORMAL               X.28 profile: 89   (14)
Port signals option:      TERM                 X.29 profile:  00   (00)
Waiting for DSS:          N (fixed)            EPOS profile: 00
Set M-bit on full Pkt:    N              Enter Data Forwarding Char: 00        (00-7F)
Max port forward limit:   NONE           Logoff Script:    0
Autoconnect:              N
Double Break:             N
Drop DSS:                 N              X.28 command:                            (32)
DSS signal:               NORMAL


_______[DynaStar _456d]_______                         Process Selections (Y/N):
Use TAB & CURSOR keys to move among entries.Press ESC to abort command and exit.
```

Figure 7-2 PAD Port Configuration Screen

5. In the **Port name** field, enter a name that will help you identify this port. This name will subsequently appear in any list of the ports, such as the list from which you select a port to configure.

6. Select appropriate values for the rest of the parameters. Parameters are explained in Table 7-2.

7. When your configuration is complete, enter **Y** in the **Process selections** field and press **<return>**.

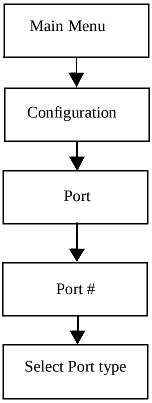


Table 7-2 PAD Port Parameter Values

Parameter	Description	Values
Port type	The type of traffic the port will handle. A menu specific to the type selected appears when the cursor is moved from the field.	Several values available. Use PAD to configure aPAD port.
Port name	A name to help you identify this port.	Max 14 chars
Connection mode	The physical level connection of the port. Dial makes the port behave as a DTE; use this selection for dial-out connections. If Dial is selected, you can define a modem initialization string. Use DCE for connecting to a terminal. Use DTE for connecting to a modem. DSS DCE and DSS DTE are used in conjunction with the Host and Incoming options (see Port Signals below) and autoconnect. Selecting these values prevents tail-ending onto the last call by guaranteeing that a new call cannot arrive at the port until the user, modem, or host computer port has acknowledged the unit's signal by dropping its own signal.	DCE (default), DTE, Dial, DSS DCE, DSS DTE
Modem speed	The line speed to the connected modem or device. Note: Auto...<CR> is a PAD command that allows the user to connect manually by entering three periods followed by a Carriage Return.	Auto (default), Auto...<CR>, 300, 600, 1200, 2400, 4800, 9600 bps, 19.2, 28.2, 33.6, 38.4, 57.6, 115.2, 230.4 kbps
Parity	Determines the parity for data sent to the terminal.	7-Auto (default), 7-Even, 7-Odd, 7-Mark, 7-Space, 8-Even, 8-Odd, 8-Mark, 8-Space, 8-None

Table 7-2 PAD Port Parameter Values (cont.)

Parameter	Description	Values
DSS flow control	Specifies that RTS/CTS data set signals be used. If DSS flow control is set to Y, the PAD forces X.3 parameters 5 and 12 to values of 0 (i.e., flow control using XON/XOFF is not possible).	Y N (default)
Call address field	Specifies how the calling address in incoming call packets is handled. If the value is Insert and the received incoming call packet does not have a calling address, the port's X.121 address is inserted. If the value is None, no action is taken.	None (default) Insert
NUI required	Specifies whether a Network User ID (NUI) is required on this port. See the section *Network User IDs* for more information.	Y N (default)
Mnemonic Type	Specifies how addresses will be handled in calls made with a mnemonic address. See the section *Call Mnemonics* for more information.	Normal (default) Secured

Table 7-2 PAD Port Parameter Values (cont.)

Parameter	Description	Values
Port signals option	Determines the way in which the port responds to port ready on the interface and to changes in the packet state of the port. The Host option is used for host computers that can place and receive calls on the same port. The Term option is used for dial-up modems, directly connected terminals, and host computers that expect leased-line signals. DTR is always up so attached modems will always answer and attached terminals and computer ports can transmit and receive. With the Modem option, the port drops its Data Set Signals for one second after a call is cleared and then brings them back up. The Incoming option is used for host computer ports and terminals that can only receive calls. Half Dup supports half-duplex signaling. To enable this feature, set Connection mode to DSS DCE and enable DSS Flow Control.	Term (default) Host Modem Incoming Half Dup
Waiting for DSS	The Waiting for Data Set Signals option prevents tail-ending onto the last call by guaranteeing that a new call cannot arrive at the port until the terminal user, modem, or host computer port has acknowledged the unit's signal drop by dropping its own signal. The available values depend on the value of Port signals option.	N Y Fixed to N for Term and Modem port signals option
Set M-bit on full Pkt	Allows a port-by-port override of the systemwide M-bit setting. When enabled, sets the M-bit on full packets to indicate they are part of a sequence.	Y N (default)

Table 7-2 PAD Port Parameter Values (cont.)

Parameter	Description	Values
Max port forward limit	Indicates when packets will be forwarded: either every 128 bytes or (if set to None) according to X.3 values.	None 128
Auto-connect	Indicates whether the PAD automatically attempts to establish a data call using a prestored X.28 selection command when a terminal makes a physical connection to the port. If Autoconnect is set to Y, the Retry Timer and Retry Attempts fields are displayed.	Y-DSS Y-CR N (default)
Double Break	When set toY, you can hit the Break key twice to escape from data mode to command mode. Equivalent to CTRL-P.	Y N (default)
Drop DSS	When enabled, the PAD port drops its data set signals for approximately 5 seconds if a successful X.25 connection has not been made within 3 minutes. The function is invoked only after an X.25 call is terminated, to allow dial modems to be released and made available for other users. The feature is usually used with the Port signals option on this menu set to TERM.	Y N (default)
DSS signal	When set to Ignore, this option allows an inbound call to the port to be accepted based on the called address without data set signals being present. This setting should be used only when specific applications that do not provide data set signals are expected to connect or attach to.	Normal (default) Ignore

Table 7-2 PAD Port Parameter Values (cont.)

Parameter	Description	Values
Retry Timer	Used on autoconnect calls to attempt to establish the data call if a previous try is unsuccessful or if an established data call is cleared. This field is displayed only when Autoconnect is set to Y.	1-255 seconds 10=default
Retry attempts	Number of times an autoconnect call attempts to establish the data call. This field is displayed only when Autoconnect is set to Y.	1-128 1=default
Port X.121 address	An X.121 address is required only if the port receives calls. The X.121 address forces an incoming call to a specific PAD port. Multiple PAD ports can share the same X.121 address to support hunt groups. See Chapter 6, *The X.25 Application*, for more information on X.121 addressing.	Max 15 BCD chars Default=null
X.121 subaddress	Defines the subaddress to be appended to the X.121 address. The subaddress consists of the last two digits of the NTN (Network Terminal Number) and can be defined as any two digits. The subaddress often corresponds to the port number.	2 digits Default=null
Use subaddress in calling DTE address	Enabling this feature causes the asynchronous port subaddress to be added to the calling address in the outgoing Call Request packet. If enabled and the length of the address is less than 14 digits, the subaddress will be appended to the address. If the address is greater than or equal to 14 digits in length, the subaddress will overwrite the last two digits of the address.	Y N (default)

Table 7-2 PAD Port Parameter Values (cont.)

Parameter	Description	Values
Inactivity timer	Clears a user's X.25 call if there is no activity (transmission or reception of data) for the specified number of minutes. This feature is used to prevent users from maintaining open channels without engaging in data exchange.	0 1-30 minutes 31-255 0=default (disabled)
X.28 Profile	Specifies one of the predefined sets of X.3 parameters for use by the local device. Press ?<return> to see a list of available profiles (names and numbers). See the section *PAD Profiles* for more information.	76-91 89=default
X.29 Profile	Specifies one of the predefined sets of X.3 parameters for use by the remote device. Press ?<return> to see a list of available profiles (names and numbers). See the section *PAD Profiles* for more information.	76-91 0=default (not used)
EPOS Profile	Modifies the pad port protocol according to the EPOS profile defined in Async Services.	00 = disabled (default) 1, 2, 3, ...
Data Forwarding Char	Defines the characters that will indicate that data should be placed in a packet and forwarded. If defined, this character is used in addition to any characters defined by X.3 parameters 3 and 4.	2 hex chars Default=null
Logoff Script	The value entered here causes the corresponding script number to be executed when the *DYNASTAR* escapes to command mode. This allows operating system commands to be executed automatically.	0-disabled, 1, 2, 3 0=default

Table 7-2 PAD Port Parameter Values (cont.)

Parameter	Description	Values
X.28 command	For autoconnect calls, the X.121 address and certain X.25 facilities can be entered in this field. Facilities entered in the field are inserted into call request packets generated by X.28 call requests and autoconnections initiated by DSS or carriage return. For manual calls, the information in this field will be prepended to your manual entry at thePAD prompt. Possible entries are X.121 address (numeric entry of up to 32 characters) Packet size (P*n*, where *n* is the maximum bytes in a packet, interpreted as a binary exponent, 2^n) $2^1 = 2$ $2^2 = 4$ $2^3 = 8$ $2^4 = 16$ $2^5 = 32$ $2^6 = 64$ $2^7 = 128$ $2^8 = 256$ $2^9 = 512$ $2^{10} = 1024$	Max 32 BCD chars Default=null See description for command syntax.

CREATING AND USING LOGOFF SCRIPTS

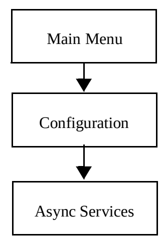
When the *DYNASTAR* is operating as a PAD, you can automatically execute previously written scripts when you escape from Data Transfer mode into command mode. The script is executed when the call clears. To create a script:

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. Select **Async Services**.

✓ The Access Server Commands menu (Figure 7-3) is displayed.




```
                    *** Access Server Commands ***


          1 - PAD configuration options
          2 - PAD profiles
          3 - X.25 Mnemonics
          4 - NUIs
          5 - Async services        (PAD, Telnet, IPX-In, SLIP)
          6 - Logoff Scripts
          7 - EPOS Profiles
          8 - Logon Screen          (Initial user screen)
          9 - Multicast Configuration


              Enter command number:

                                    Process selections (Y/N): Y

_________[DynaStar_3df2]__________
Terminate input with <RET>.                 Press ESC to return to previous menu.
```

Figure 7-3 Access Server Commands Menu

3. Select **Logoff Scripts**.

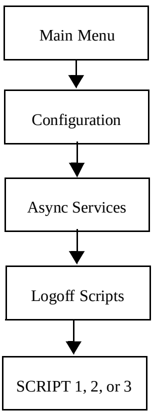
4. From the list that appears, select **SCRIPT1**, **SCRIPT2**, or **SCRIPT3**.

✓ A menu similar to Figure 7-4 is displayed.

5. Fill in up to three valid command lines in the spaces provided and indicate the delay between each command (0 to 6 seconds).

6. Select **Y** in the Process selections field and press **<return>**.

7. To activate a particular script, enter its number in the **Logoff Script** field on thePAD Port Configuration screen (Figure 7-2). A zero in this field disables the script feature.




```
                         *** LOGOFF Script 1 ***

                                        Last changed:  4-13-02 23:44:23
LINE1:                                                   (16 hex characters)
PAUSE1:              0                   (toggle value between 0-6 seconds)
LINE2:                                                   (16 hex characters)
PAUSE2:              0                   (toggle value between 0-6 seconds)
LINE3:                                                   (16 hex characters)
PAUSE3:              0                   (toggle value between 0-6 seconds)



 _________[DynaStar_3df2]__________             Process selections (Y/N): Y
 Use TAB & CURSOR keys to move among fields.  Press ESC to abort command & exit.
```

Figure 7-4 PAD Logoff Script Screen

■ PAD PROFILES

Profiles are predefined sets of X.3 parameters that are designed to be used with specific types of asynchronous devices. Each profile is identified by a number and, optionally, a name. The *DYNASTAR* has two built-in profiles defined by the ITU-T that cannot be changed: the transparent profile (91) and the simple profile (90). There are an additional 14 profiles (numbered 76 through 89) that you can configure. Four of these profiles are predefined: one for display devices

(CRT), one for printing terminals (TTY), one for Telnet clients (TELNET), and one for an X.29 set command for a LAN (LAN). The remaining 11 are set to default values that match the CRT profile.

NOTE: For convenience, all profiles can be referenced by a second set of numbers, from 1 to 16, as indicated on the PAD Profiles screen (Figure 7-5).

The PAD Port Configuration screen (see Figure 7-2) lets you define an **X.28 profile** (local profile) and an **X.29 profile** (remote profile) for the port you are configuring. The values in the X.28 profile govern the internal operation of the local PAD port.

The X.29 profile, if defined, governs the operation of the remote PAD port. When a call is initiated, the local PAD port sends an X.29 data packet to the device at the distant end requesting a change in the X.3 parameters to match the profile listed in this field.

You can temporarily override the local profile set for your port with the X.28 PROF command, and you can use the X.28 SET or SET? commands to temporarily change individual X.3 parameters.

The procedure below explains how to configure profiles:

1. From the Main menu, select **Configuration**.

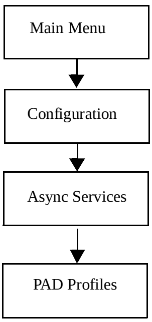
✓ The Configuration Commands menu (Figure 3-11) appears.

2. Select **Async Services**.

✓ The Access Server Commands menu (Figure 7-3) appears.

3. Select **PAD profiles**.

✓ The PAD Profiles menu, shown in Figure 7-5, appears. (The fields in this menu are described in Table 7-3.)




```
                              ***PAD Profiles***
                                            Last changed:  1/1/99  17:00:44
   Built-in    91 (16) - TRANS     CCITT transparent
   profiles:   90 (15) - SIMPLE    CCITT simple

   Profile Name      Profile # for          Optional Description
   (1-8 chars)       Initial Values         (up to 32 characters)
89 (14) - CRT        90 (15)            Display terminal
88 (13) - TTY        90 (15)            Printing terminal
87 (12) - TELNET     91 (16)            Telnet client
86 (11) - LAN        91 (16)            LAN X.29 SET
85 (10) -            89 (14)
84 (09) -            89 (14)
83 (08) -            89 (14)
82 (07) -            89 (14)
81 (06) -            89 (14)
80 (05) -            89 (14)
79 (04) -            89 (14)
78 (03) -            89 (14)
77 (02)-             89 (14)
76 (01) -            89 (14)
                          Enter profile number to view/change X.3 parameters:
_______[DynaStar _456d]_______                  Process Selections (Y/N):Y
Profile name must not start with number.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 7-5 PAD Profiles Menu

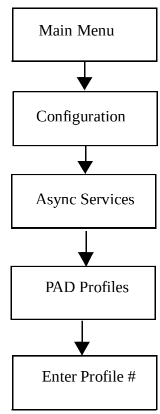
4. Next to the number of the profile that you want to configure, enter a short name for the profile.

5. In the **Profile # …** column, enter the number of an existing profile that is the most similar to the profile that you want to configure. (Appendix D, *X.3 Profiles and Parameters*, lists the values of the default profiles.) This profile will be used as the starting point for the new profile.

6. In the **Optional Description** column, enter a description that will help you identify the function of this profile.

7. In the **Enter profile number to view/change X.3 parameters** field, enter the number of the new profile that you are defining and press **<return>**.

✓ The X.3 Parameter Values screen appears, as shown in Figure 7-6.



X.3 Parameter Values

Profile 89 (14) CRT	Enter value	Permitted values
1: PAD recall	1	0-no escape, 1-DLE, 32-126 define char
2: PAD echo	1	0-no echo, 1-echo
3: Data forwarding chars	2	0, 1, 2, 4, 8, 16, 32, 64, 128, 3-255
4: Idle timer	0	0-disabled, 1-250 twentieths of a second, 251-3 to 10ms, 252-10ms, 253-30 ms 254-40ms, 255-50ms
5: Flow control by PAD	1	0-no use of XON/XOFF, 1-use XON/XOFF
6: PAD service signals	5	0-none, 1-no prompt, 5-prompt & *, 8-15
7: Break handling	0	0, 1, 2, 5, 8, 21
8: Discard output	0	0-normal delivery, 1-discard
9: Padding after CR	0	0-none, 1-255 padding characters
10: Line folding	0	0-none, 1-255 graphic characters per line
12: Flow control of PAD	1	0-no use of XON/XOFF, 1-use XON/XOFF
13: LF after CR	4	0, 1, 4, 5, 6, 7
14: Padding after LF	0	0-none, 1-255 padding characters
15: Editing	1	0-none, 1-editing in data transfer
16: Character delete	127	0-126 IA5 character, 127-DEL
17: Line delete	24	0-23 & 25-127 IA5 character, 24-CAN
18: Line display	18	0-17 & 19-127 IA5 character, 18-DC2
19: Editing signals	2	0-none, 1-printing, 2-display terminal
20: Echo mask	240	0, 1, 2, 4, 8, 16, 32, 64, 128, 3-255
21: Parity treatment	3	0-none, 3-checking and generation
22: Page wait	0	0-disabled, 1-255 LFs

Press ESC to abort command & exit. Process Selections (Y/N):

Figure 7-6 X.3 Parameter Values Screen

8. Change the parameters as required by entering the new value in the **Enter value** column of the appropriate parameter. Press <**tab**> or <**return**> to go to the next field. You will not be allowed to enter an invalid value.

9. When you have made the necessary changes, enter **Y** in the **Process Selections** field and press <**return**>.

NOTE: The X.3 parameters are ***NOT*** saved until step 10 below is completed.

✓ You return to the PAD Profiles menu.

10. When you have completed your configuration, enter **Y** in the **Process Selections** field and press <**return**>.

NOTE: You must save your changes on *both* screens for your changes to take effect.

Table 7-3 PAD Profiles Menu Fields

Field	Description
Built-in profiles	Lists the two ITU-T (CCITT) defined profiles that are available in the *DYNASTAR* (91 [transparent] and 90 [simple]). These profiles cannot be changed.
Profile Name	The profile name is optional; it provides a brief identification for the profile. The name can also be used in the X.28 PROF command instead of the profile number.
Profile # for Initial Values	The profile number that you use as the basis for setting the X.3 parameters. If the profile named in this column is later changed or deleted, the parameters for this profile do not change.
Optional Description	This field is optional and can be used to enter up to 32 characters describing the device that uses the profile or the circumstances under which you use the profile.

■ Network User Identification

The Network User Identification (NUI) facility is supported for PAD ports. The NUI is much like a password and can be used as a security mechanism to verify that only authorized callers are placing calls.

If the NUI option is enabled for a port, all outgoing calls on this port will require an NUI in the call request packet. The *DynaStar* compares the NUI entered by the user to the entries in the NUI table before it sends the call out to the network. If the entered NUI does not match an entry in the NUI table, the *DynaStar* refuses to place the call and returns an error message to the PAD screen. If the NUI does match an entry in the NUI table, the *DynaStar* places the NUI in the user data field of the call request packet and then sends the call out to the network. A maximum of 50 NUIs can be defined in the *DynaStar*.

To define an NUI:

1. From the Main menu, select **Configuration**.

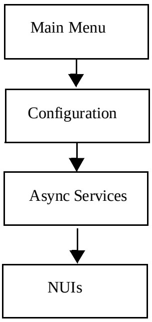
✓ The Configuration Commands menu (Figure 3-11) appears.

2. Select **Async Services.**

✓ The Access Server Commands menu (Figure 7-3) appears.

3. Select **NUIs**.

✓ The Network User IDs screen, shown in Figure 7-7, appears.




```
                    ***Network User IDs***
                     Last changed:  6-4-02  17:00:44
                 Enter the X.121 address for each NUI
     NUI (16 chars)                          X.121 Address
1:
2:
3:
4:
5:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:
16:

_______[DynaStar _456d]_______                  Process selections (Y/N):Y
To change or add entry, enter new value.           Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 7-7 NUI Definition Screen

4. Enter the NUI in the **NUI** column. (This is the string that the user will enter.)
5. In the **X.121 Address** column, enter the called X.121 address associated with the NUI.
6. When you have finished defining all NUIs, enter **Y** in the **Process selections** field and press **<return>**.

To place an X.25 call with an NUI, enter the letter N, the NUI, a dash, and the called address. To ensure password integrity and prevent potential eavesdroppers from deciphering the NUI, the string entered after the letter N is not echoed to the screen. For example:

NDAVES-1234

places a call to X.121 address 1234 with the NUI *DaveS*.

■ CALL MNEMONICS

Call mnemonics (also called abbreviated addresses) let you connect to a remote destination by entering a meaningful name rather than an X.121 numeric address.

Call mnemonics have been implemented with two options: **Normal** and **Secured**. In **Normal** mode, the PAD port replaces the mnemonic name with the equivalent X.121 address and then places the X.25 call. In **Secured** mode, the X.121 address again replaces the mnemonic name, but, in addition, the calling address is also placed in the X.25 call packet. The calling address can then be used by the destination for security checking. You select **Normal** or **Secured** mode in the **Mnemonic Type** field of the PAD Port Configuration menu, as shown in Figure 7-2. The default value is **Normal**.

To define a call mnemonic:

1. From the Main menu, select **Configuration**.

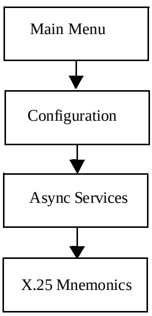
✓ The Configuration Commands menu (Figure 3-11) appears.

2. Select **Async Services**.

✓ The Access Server Commands menu (Figure 7-3) appears.

3. Select **X.25 Mnemonics**.

✓ The Mnemonic Address screen, shown in Figure 7-8, appears.




```
                    ***Mnemonics Address/X.121 Address Mapping***
                                            Last changed:  10/21/98  17:00:44

        Mnemonics              Called        Calling          Max. Sessions
      (16 characters)         (15 BCD)      (15 BCD)          (0-255 or ^D)

1:
2:
3:
4:
5:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:
16:

_______[DynaStar _456d]_______                       Process selections (Y/N):Y
To change or add entry, enter new value.             Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move fields.         Press ESC to return to previous menu
```

Figure 7-8 Mnemonics Definition Screen

4. In the Mnemonics Address screen, enter the destination mnemonic in the **Mnemonics** column.

5. In the **Called** column, enter the destination address.

6. If you are using **Secured** mode (set in thePAD Port Configuration screen), enter the calling address to be used for this destination in the **Calling** column.

   NOTE: The root operator can fill in the called and calling X.121 addresses and leave the **Mnemonics** field blank. A lower level operator with write permissions could then fill in a meaningful name at a later time. This operator can modify the name field but cannot view the associated called and calling addresses. If he defines a name for an entry that has no addresses configured, the addresses in the first table entry will be copied to that entry. If an operator with read permission accesses the menu, he can view the mnemonics but he does not see the addresses.

7. In the **Max. Sessions** column, enter the maximum number (from 1 to 255) of concurrent calls allowed using this mnemonic. CTRL-D or a blank entry means an unlimited number of calls; a zero inhibits the use of call mnemonics to this destination.

8. When you have entered all the mnemonics, enter **Y** in the **Process selections** field and press **<return>**.

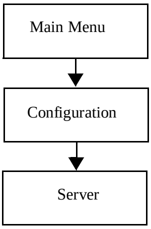
To place a call with a mnemonic, type a period followed by the mnemonic at the PAD prompt. For example (the * is the PAD prompt):

*****.DALLASHOST

PRIORITY LCNS

The call mnemonics table holds a maximum of 200 entries. The first 10 entries in this table can be reserved for priority mnemonics. When this option is set, the system reserves one LCN for the first 10 entries in the mnemonics table. Other calls cannot be established if there are fewer than 10 available LCNs.

You configure whether or not you want to use reserved LCNs in the Systemwide Parameters screen (Figure 7-9). By default, **Reserved LCNs** is set to **N**.




```
                    *** Systemwide Parameters***
                                        Last changed: 4-23-02  7:00:45

Server name: DynaStar399c                                          (47)
Supervisor console herald:      DynaStar Supervisor                (32)
Dial IP traffic idle timer:     2      (0-disable, 1-254 min), 255-10 sec
Dial IPX traffic idle timer:    2                  (0-disable, 1-255 min)
Dial Bridge traffic idle timer: 2                  (0-disable, 1-255 min)
B Channel call timeout:         60                (0-disable, 1-1440 min)
X.25 call set-up retry timer:   1                              (1-30 min)
XOT Idle Timer                  0                   (0-disable, 1-30 min)
PPP IP traffic prioritization:  0                       (0-disable, 1-99)
IPX-In preferred File Server:                                      (47)
IPX-Out broadcast address:      399c                                (8)
Reserved LCNs:                  N                          <CR> to toggle
Exhaustive Routing:             N                          <CR> to toggle
X32 No LCN Drop Timer:          6                  (0-disable, 1-12(10sec))
Daughter Board Auto-Recover     Y                          (CR) to toggle



_______[DynaStar 399c]_______                 Process selections (Y/N): Y
Use TAB & CURSOR keys to move fields. Press ESC to return to previous menu
```

Figure 7-9 Systemwide Parameters Screen

■ VIRTUAL PORT CONFIGURATION

In addition to the physical PAD port connections, you can configure up to 32 virtual PAD connections. For this type of configuration, the *DYNASTAR* acts as a terminal server for the virtual connections.

All virtual ports currently share the same PAD configuration, which is defined on thePAD Port Configuration screen. To configure a virtual PAD port:

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu appears.

2. Select **Port**.

✓ A list of available ports appears.

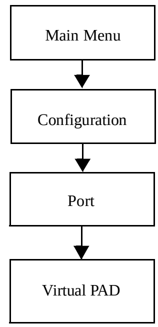
3. Select the **Virtual PAD** port.

✓ The PAD Port Configuration screen, as shown in Figure 7-10, appears. This screen is similar to the PAD

Port Configuration screen for physical PADs, but it has fewer parameters.

```
                        ***PAD Port Configuration***
Port 10                                         Last changed: 4-23-02  17:00:44

 |---  Press <RET> to toggle values  --| |--- Type in values.  Max chars shown in ()  ---|
 Port type:     Virtual PAD                   Port name:         Virtual PAD              (14)

                                              Port X.121 address:                   (15 BCD)
                                              X.121 sub-address:                     (2 BCD)
                                              Use sub-address in calling DTE address: N
                                              Inactivity timer: 0          (0-disable, 1-30 min)
Call address field:         None
NUI Required:               N
Mnemonic Type:              Normal
                                              Enter ? <RET> for profile list
                                                    X.28 profile: 89   (14)
                                                    X.29 profile:  00   (00)

Set M-bit on full Pkt:      N                 Enter Data Forwarding Char: 00        (00-7F)
Max port forward limit:     NONE

Drop DSS:                   N
DSS signal:                 NORMAL

_______[DynaStar _456d]_______                         Process Selections (Y/N): Y
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 7-10 Virtual PAD Port Configuration Screen



4. Configure the parameters as required by your network. (Parameters are described in Table 7-2.)

5. When your entries are complete, enter **Y** in the **Process selections** field and press **<return>**.

■ INTERNAL MODEM INTERFACE

The *DYNASTAR 100e* and *DYNASTAR 2000* models are available with an optional V.90 internal modem WAN interface for remote dial in/out access. This is especially useful for remote dial-up connections, via the PSTN, to the diagnostic (console) port for provisioning or troubleshooting. See Chapter 2, *Installation*, for more information about the physical interface.

Configuration of the interface is similar to configuration of a PAD port.

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu appears.

2. From the Configuration Commands menu, select **Port**.

✓ A list of available ports appears.

3. Enter the number of the modem port.

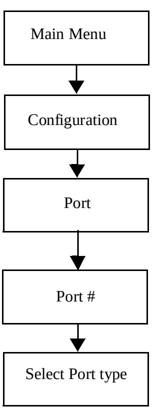
✓ The Port Configuration screen appears.

4. Toggle the **Port Type** field until **PAD** appears.

✓ A screen similar to the one shown in Figure 7-11 appears.

5. Change the default settings if required. However, the screen defaults to the correct settings to allow a dial-up PSTN connection to a PAD prompt.

6. When your configuration is complete, enter **Y** at the **Process Selections** prompt and press **<return>**.




```
                         ***PAD Port Configuration***
Port 4   MODEM module                          Last changed:  5-29-02  17:00:44

 |---  Press <RET> to toggle values  --| |--- Type in values.  Max chars shown in ()  ---|
Port type:      PAD                    Port name:      MODEM 1                      (14)

Connection mode:    DCE         Port X.121 address:                             (15 BCD)
Modem speed:        9600 baud   X.121 sub-address:                               (2 BCD)
Parity:             7-EVEN      Use sub-address in calling DTE address: N
DSS flow control:   N           Inactivity timer: 0          (0, 1-30 min, 31-255 out)
Call address field: NONE
NUI Required:       N           Enter ? <RET> for profile list
Mnemonic Type:      NORMAL                 X.28 profile: 89   (14)
                                           X.29 profile:  00   (00)
                                           EPOS profile: 00
Set M-bit on full Pkt:  N       Enter Data Forwarding Char: 00                  (00-7F)
Max port forward limit:NONE     Logoff Script:     0
Autoconnect:        N
Double Break:       N
                                X.28 command:                                      (32)
                                Modem cmd:AT&FS0=1E1Q0V1X4&C1&D2&K3  (30)

_______[DynaStar _456d]_______                     Process Selections (Y/N):
Use TAB & CURSOR keys to move among entries.Press ESC to abort command and exit.
```

Figure 7-11 PAD Port Configuration Screen for MODEM Interface

■ PLACING A CALL FROM A PAD

Place a call using the X.121 address of the destination. You may include certain facilities and up to 12 characters of user data in the call request. Valid facilities are defined in Table 7-4. The format for a call is as follows:

facility, facility -X.121address Duserdata

or

facility, facility -X.121address Puserdata

where:

facility is a single letter code in some cases followed by a parameter as defined in Table 7-4. More than one facility can be specified, as long as they are separated by commas.

X.121address is the destination X.121 address. If facilities are included in the call request, the X.121 address must be preceded by a dash.

D or *P* indicates that up to 12 ASCII characters that follow are to be sent as call user data.

NOTE: If abbreviated addresses have been configured (see the earlier section *Call Mnemonics*), simply type the name of the service you want to connect to, preceded by a period (.), and the *DYNASTAR* will translate the name to the assigned X.121 address.

Table 7-4 Valid Facilities for PAD Cal l

Facility Code	**Definition**	**Valid Parameter Values**
C	Charge information	No parameter
D	Throughput class negotiation	3 through 12 (decimal)
G	Closed User Group (CUG)	01 to 99 (decimal)
N	Network User Identification (NUI)	ASCII string, maximum 16 characters

Table 7-4 Valid Facilities for PAD Cal l(cont.)

Facility Code	Definition	Valid Parameter Values
P	Packet size negotiation	4 to 10 (decimal number representing 2^n). See Table 7-2 for expanded values.
R	Reverse charging	No parameter
T	RPOA transit network selection	4 decimal digits
W	Window size negotiation	1 to 7 (decimal)

■ PAD COMMANDS AND SERVICE SIGNALS

ITU-T Recommendation X.28 defines the commands that a user enters to request services from a PAD and the service signals that are received in response to those commands. It also defines unsolicited service signals that report events, such as call clearing.

The *DYNASTAR* supports all defined X.28 commands, all defined X.28 service signals, and *DYNASTAR* extensions to X.28. Table 7-5 summarizes the X.28 PAD commands that are available.

To use any of these commands except **<Ctrl>-<P>**, type the command at thePAD prompt (* is the default prompt) and press **<return>**.

For detailed information on these commands, refer to ITU-T Recommendation X.28.

Table 7-5 PAD Commands and Service Signals

Command	PAD Function	When Used
Ctrl-P	Used in Data Transfer mode to put the port in Command Mode. <CR> on a line by itself returns the unit to Data Transfer Mode.	When call is up.

Table 7-5 PAD Commands and Service Signals (cont.)

Command	PAD Function	When Used
CLR	Clears a virtual call.	When call is up.
INT	Sends an interrupt.	When call is up.
PROFn	Assigns the PAD a standard set (n) of parameter values.	When call is up or in Command Mode. If applied when call is up, profile is used only for the duration of the call.
PAR?x,x,x	Requests a list of the current values of specified parameters, where each x represents an individual parameter. If x is not specified, returns all X.3 parameters.	When call is up or in Command Mode.
QUIT	Causes the port's data set signals to drop for 5 seconds. If the port is configured as a DCE, DSR and DCD are dropped. If the port is configured as a DTE, DTR is dropped.	In Command Mode. Call must be cleared for Quit command to be valid.
RESET	Resets a virtual circuit.	When call is up.
SETx:y	Sets X.3 parameter x to value y.	When call is up or in Command Mode. If applied when call is up, parameter setting is used only for the duration of the call.
SET?x	Sets the specified X.3 parameters and lists them after they are set.	When call is up or in Command Mode. If applied when call is up, parameter setting is used only for the duration of the call.
STAT	Reports the status of the line.	When call is up or in Command Mode.

PAD Clearing Causes

Table 7-6 lists the clearing causes that are included in a Clear Request. These messages appear on the user's screen.

Table 7-6 Clearing Causes

Clear Cause	Meaning
CLR OCC	Busy
CLR NC	Network Congestion
CLR INV	Invalid Call
CLR NA	Access Barred
CLR ERR	Local Procedure Error
CLR RPE	Remote Procedure Error
CLR NP	Illegal Address
CLR DER	Out of Order
CLR DTE	Disconnected
CLR RNA	Refused Collect Call

In addition to the standard X.28 clearing causes, the *DynaStar* supports two extensions:

CLR IDLE — The data inactivity timer (localPAD parameter 127) has expired and the PAD has cleared.

CLR SERV — The service console has disabled either the terminal's port or the network's access port.

The Frame Relay Application

■ Overview

Frame relay is designed to provide high speed data transmission with minimal delay and efficient use of bandwidth. The *DynaStar* provides frame relay bridging, routing, and switching and can establish a link over a frame relay line to any distant router that can be reached through the frame relay network. Requirements for the distant router, based on the application traffic carried on the link, are summarized in Table 8-1.

Table 8-1 Remote Router Requirements

Application	Distant Device	Protocol Compliance
IPX Router	*DynaStar*	RFC 1362
IP Router	Any IP Router	RFC 1490
Ethernet Bridge	Any Ethernet Bridge	IEEE 802.1d, RFC 1294
X.25 over Frame Relay	Any compatible device	RFC 1490

Frame relay allows a single physical line to be divided into multiple logical connections. A unique identifying number, called a Data Link Connection Identifier (DLCI), is assigned to each logical connection. Each DLCI can be independently configured to support any combination of IP, IPX, or Bridge traffic, or it can be configured to provide frame relay-to-frame relay switching or X.25 over frame relay. Once configured and initialized, the line is ready for use. No user interaction is required and the line will not disconnect under normal operating conditions.

The *DynaStar* supports Implementation Agreement FRF.12 for End-to-End or UNI/NNI fragmentation. By controlling delay variations, fragmentation allows real-time traffic such as voice to share connections with data traffic. End-to-End

fragmentation, controlled on the Frame Relay Switching, Routing, and Bridging menu, allows frames to be fragmented on a per-PVC basis. UNI/NNI fragmentation, controlled on the Frame Relay Port Configuration menu, fragments all frames on the interface.

The *DynaStar* can reroute IP traffic carried over frame relay if the frame relay line goes down by automatically setting up a specified PPP dial connection. Using LMI management, the *DynaStar* can also switch traffic for an individual DLCI to a backup frame relay or ISDN route when the DLCI goes down and return the primary route to service when it again becomes active.

The *DynaStar* can transport X.25 over frame relay. X.25 over Frame Relay is described later in this chapter. In addition, the *DynaStar* can use HDLC connections over TCP/IP to carry frame relay traffic, as described in Chapter 6, *The X.25 Application*.

■ Frame Relay Port Configuration

To use frame relay to connect to an outside network or to use it as the underlying protocol for bridge or router traffic, you must first configure at least one of the WAN ports in your *DynaStar* to support frame relay. A complete description of the frame relay port configuration parameters is given in Table 8-2.

1. From the Main menu, select **Configuration**.

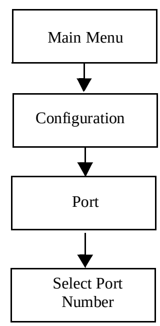
✓ The Configuration Commands menu (Figure 3-11) appears.

2. Select **Port**.

✓ A list of available ports appears.

3. Select the port that you want to configure with the frame relay protocol and enter that port's number in the **Enter port number** field.

NOTE: You must select a port that is capable of handling the frame relay protocol. These



ports are the baseboard ports labeled HS WAN and Sync/Async or any port on the QUAD, 8-port, or 16-port boards.

✓ A menu showing the port parameters that are currently set for the port appears.

4. If the port is not currently configured as frame relay, toggle the **Port type** field until **frame relay** appears and press **<tab>**.

✓ The screen displays the parameters that need to be configured for frame relay, as shown in Figure 8-1.

```
                         ***Frame Relay Port Configuration***
 Port:  8  IS-35                                      Last changed:  5-22-02  11:26:45

    |---  Press <RET> to toggle values  --||--- Type in values.  Max chars shown in ()  ---|
Port type:        frame relay                      Port name:   HS WAN                (14)

Connection mode:        DTE

Line speed:             56.0 kbps
DLCI management:        LMI                         User, Network, or NNI: USER
Circuit backup:         N

Traffic types permitted on line:
          IP Routing:             Y
          IPX Routing:            Y
          Ethernet Bridging:      Y

UNI/NNI Fragementation:  NONE



 _________[DynaStar_3614]__________                  Process selections (Y/N): Y
  UseTAB & CURSOR keys to move among fields.   Press ESC to abort command & exit.
```

Figure 8-1 Frame Relay Port Configuration Screen

5. In the **Port name** field, enter a name that will help you identify this port. This name will subsequently appear in any list of the ports, such as the list from which you select a port to configure.

6. Enter the connection mode for this line. **DTE** means that the port is a physical DTE device looking for an external clock source. **DCE** means that the port is a physical DCE that provides clocking.

7. Select the **DLCI Management** type and specify **User**, **Network**, or **NNI** (see Table 8-2).

8. If IP traffic being carried over the frame relay line is to be backed up by a PPP dial line when the frame relay line goes down, select **Y** for **Circuit backup**.

   NOTE: Be sure **N** is selected for **Circuit backup** if any of the DLCIs for this frame relay port are to be backed up individually. (See *Frame Relay Backup over Frame or ISDN* later in this chapter for more information on this feature.)

9. If you enabled **Circuit backup**, additional fields appear on the screen. Configure these to indicate when to back up and restore the line and to identify the backup line.

10. Select the traffic types to be permitted on the line in the **Traffic types…** field.

11. If UNI/NNI fragmentation is to be used to fragment all frames on this interface, enter the number of bytes in each fragment, not including the four byte header.

    NOTE: End-to-End fragmentation is enabled on the Frame Relay Switching, Routing, and Bridging menu as described in the next section.

12. When your configuration is complete, enter **Y** in the **Process selection** field and press **<return>**.

Table 8-2 Frame Relay Port Parameter Values

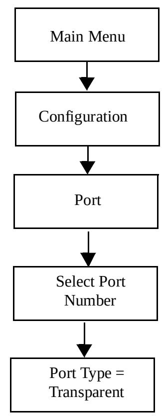
Parameter	Description	Values
Port type	The type of traffic the port will handle. <return> toggles through permissible values. A menu specific to the type selected appears when the cursor is moved from the field.	Various, select *frame relay* for a frame relay port.
Port name	A name to help you identify this port.	Max 14 chars
Connection mode	The physical level connection of the port. DCE means that the port is a physical DCE that provides clocking. DTE means that the port is a physical DTE device looking for an external clock source.	DTE (default) DCE
Line speed	The speed of the line (interface dependent).	1200 bps - 2.048 Mbps 56k=default
DLCI management	Specifies the standard to be used for the frame relay implementation. CCITT supports Q.922; ANSI supports Annex D of T1.617. *Note*: LMI should be selected if the DLCI is to be backed up over a frame relay or ISDN connection.	LMI (default) CCITT ANSI None
User, Network, or NNI	This parameter lets you select LMI User, LMI Network, or LMI Network-to-Network (NNI) as the implementation. This indicates which side initiates the poll. When NNI is selected, polling occurs in both directions.	User (default) Network NNI

Table 8-2 Frame Relay Port Parameter Values (cont.)

Parameter	Description	Values
Circuit backup	Should be enabled only if IP traffic carried over frame relay is to be rerouted to a a dial line if this line goes down. If enabled, the parameters Backup when line down, Restore when line up, and Backup location name also appear on the screen. *Note*: This parameter should be disabled if any DLCI on this line is being backed up individually from the Frame Relay Backups & Connections Properties menu (as described later in this chapter).	Y N (default)
Backup when line down	Specifies how quickly this line should be backed up if it goes down. Appears only if Circuit backup is set to Y.	1-255 seconds 10=default
Restore when line up	Specifies how quickly the backup line should be taken down and this line restored once this line comes back up. Appears only if Circuit backup is set to Y.	1-255 seconds 30=default
Backup location name	Identifies the line that will be used as the backup line if the frame relay line goes down. This line must be configured in the PPP dial directory (see Chapter 10, *The PPP Application*).	17 characters Default=null
Traffic types permitted on line	Indicates whether IP, IPX, and/or Ethernet bridged traffic are allowed on this frame relay line.	Y (default) N
UNI/NNI Fragmentation	Determines the number of bytes per fragment (not including FRF.12 or Q.922 address octets) when UNI/NNI fragmentation is used. *NOTE*: End-to-End fragmentation is enabled and fragment size is set on the Frame Relay Switching, Routing, Bridging, and SNA Table described later in this chapter. See also Table 8-3, *Frame Relay Connection Parameters*.	NONE (disabled; default) 1 to 1500 bytes

TRANSPARENT PORT TYPE

The MCS-11 and SES-91 bit protocols are supported on the sync/async and WAN ports and on the QUAD board. The protocols are tunneled over frame relay using the port and DLCI configured in the port configuration screen. Use the *Transparent* port type to configure this type of port. Figure 8-2 shows the Transparent Port Configuration screen.




```
                    ***Transparent Port Configuration***
Port:  3  IS-232                                  Last changed:  6-6-02  11:26:45

   |---  Press <RET> to toggle values  --||--- Type in values.  Max chars shown in ()  ---|
Port type:       Transparent                      Port name:   sync/async           (14)

Connection mode:        DTE                       Frame Relay port:      3
Line speed:             9.6 kbps                  Frame Relay DLCI:   100
Protocol:               MCS-11
Line Idle::             0

________[DynaStar_3614]_________                  Process selections (Y/N): Y
 Use TAB & CURSOR keys to move among fields.   Press ESC to abort command & exit.
```

Figure 8-2 Transparent Port Configuration Screen

■ FRAME RELAY CONNECTIONS

Once the frame relay line or lines are configured, you can configure the switched, bridged, or routed frame relay connections. These connections are based on the frame relay DLCI. The DLCI is similar to an X.25 LCN and is used to provide a logical identification for a connection. Since frame relay uses semi-permanent connections, you must indicate which port and DLCI to use for a given connection. Two DLCIs are required for a switched frame relay connection. A single DLCI is used for a connection terminating at the *DYNASTAR*. A maximum of 1024 DLCIs are available.

8

The Frame Relay Application

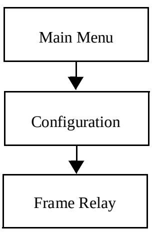
The procedure for configuring frame relay connections is given below. All parameters in the Frame Relay table are described in Table 8-3.

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands screen (Figure 3-11) is displayed.

2. Select **Frame Relay**.

✓ The Frame Relay Parameters screen, as shown in Figure 8-3, is displayed.



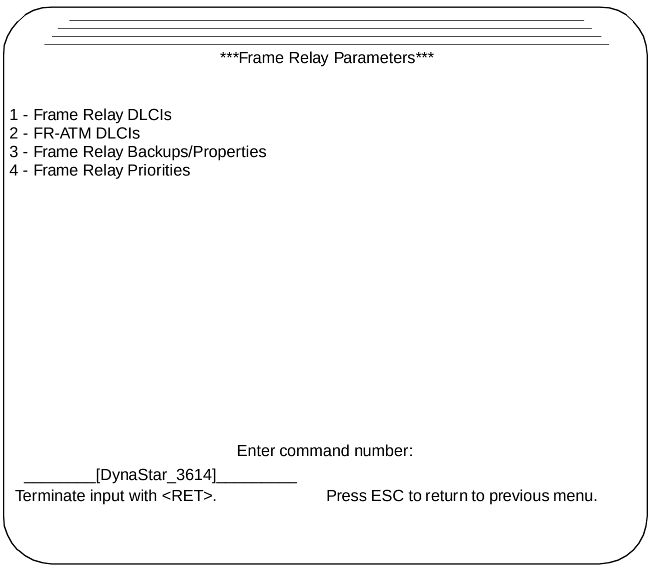
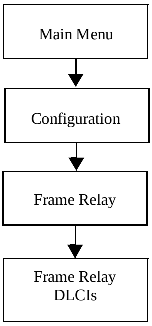


Figure 8-3 Frame Relay Parameters Menu

3. Select **Frame Relay DLCIs**.

✓ The Frame Relay DLCI Configuration Table (Figure 8-4) is displayed.

4. In the **Type** column, toggle to select the type of connection. For Router/Bridge traffic, select **RFC 1490**. For Switched traffic, select one of the other choices.



5. For both Switching and Router/Bridge traffic, configure the port and DLCI that the incoming call will use in the **Source Port/DLCI** columns.

6. For Switching traffic only, configure the outgoing port and DLCI that the call should use in the **Dest Port/DLCI** columns.

7. For Router/Bridge traffic, indicate whether IP, IPX, and/or Bridged traffic will be allowed on this connection in the **IP**, **IPX**, and **B** columns.

```
                    ***Frame Relay DLCI Configuration Table***
                                               Last changed:  9-23-02  11:26:45

               Source      Dest                          CIR     Fragmnt
 Type          Port  DLCI  Port   DLCI IP  IPX  B  PRTY  Kbps    Bytes  Dest IP Address
1RFC 1490       5     16               Y   Y    Y    1    19.2k  NONE   0.0.0.0
2Switched       3    100    5     17
3
4
5
6
7
8
9
10
11

 ________[DynaStar_3614]_________              Process selections (Y/N): Y
Use <CTRl-D> to delete entry                 <RET> to toggle or type value
Use <TAB> and CURSOR to move fields           Press ESC to return to previous menu
```

Figure 8-4 Frame Relay DLCI Configuration Table

8. Indicate the priority of the call in the **PRTY** column.

9. In the **CIR** field, indicate the Committed Information Rate for this call. This parameter is used to rate limit data out to the Frame Relay network.

10. If End-to-End fragmentation is to be used for this PVC, enter the number of bytes per fragment, not including the four-byte header.

NOTE: UNI/NNI fragmentation is enabled on the Frame Relay Port Configuration menu as

described in the next section.

11. For IP traffic, indicate the destination IP address in the column of the same name.
12. When your configuration is complete, enter **Y** in the **Process Table selections** field and press **<return>**.

Table 8-3 Frame Relay Connection Parameters

Parameter	Description	Values
Type	The type of connection that will be allowed. For Router/Bridge traffic, select RFC 1490. For switched traffic, select Switched, Annex G, or Broadcst. Broadcst allows broadcast capability from one frame relay port to another. TRANS-FR and PAD-FR are explained in Chapter 19.	Switched RFC 1490 Annex G TRANS-FR PAD-FR Broadcst
Source Port and DLCI	The frame relay port and DLCI the traffic will use as it enters the *DYNASTAR*.	Any frame relay port 16-1022 for DLCI
Dest Port and DLCI	Applies only when Type is set to Switch. The frame relay port and DLCI the traffic will use as it exits the *DYNASTAR*.	Any frame relay port 16-1022 for DLCI
IP	Applies only when Type is set to RFC1490. If set to Y, IP traffic is enabled. A valid IP address must also be entered.	Y N
IPX	Applies only when Type is set to RFC1490. If set to Y, IPX traffic is enabled.	Y N
B	Applies only when Type is set to RFC1490. If set to Y, Bridge traffic is enabled.	Y N

Table 8-3 Frame Relay Connection Parameters (cont.)

Parameter	Description	Values
PRTY	Determines priority to be given to the call. Priority ranges from 0 to 5. See *Prioritization* later in this chapter for more information.	0-5 1 = default
CIR	The Committed Information Rate for the frame relay traffic. This is the transfer rate that the frame relay network is committed to transfer under normal operating conditions. See *Prioritization* later in this chapter for more information.	Any value in 1 kbps increments
Fragment Bytes	Number of bytes per fragment (not including FRF.12 or Q.922 address bytes) for this PVC when End-to-End fragmentation is used. Note: When UNI-NNI fragmentation is used, fragment size is set on the Frame Relay Port Configuration menu.	NONE (disabled; default) 1 to 1500 bytes
IP Address	Applies only when Type is set to RFC1490 and IP is set toY. Indicates the destination IP network.	Any valid IP address

Prioritization

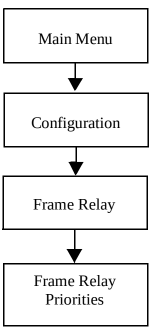
Through the judicious use of the CIR, fragmentation, and priority parameters, you can carefully manage the traffic so that no application is starved of bandwidth and time-critical requirements are met even under conditions of heavy load.

The CIR parameter lets you allocate bandwidth between multiple frame relay DLCIs on a port. If a port has 56k bandwidth available, this can be allocated between multiple DLCIs. For example, you could limit IP traffic to 28kbps, leaving 28kbps for other traffic, including time-critical SCADA traffic and management frames (LMI). When you

configure a CIR for a DLCI, the traffic is shaped so that the DLCI uses its bandwidth allocation over time, not in bursts of heavy activity. This ensures that time-critical traffic is not help up in the network behind a burst of other traffic.

The priority parameter ranges from 0 to 5. You can toggle it from 1 to 5 (1 is the default), and also type in 0. Frames with a 0 priority have the highest priority. Normally, this is reserved for frame relay management frames (LMI), but it can also be used for limited amounts of time-critical frames.

The priority weighting between each priority level is normally set at 2. This means that two higher priority frames are sent for each lower priority frame (except for 0, which always goes first). You can configure this weighting from the Frame Relay Priority Weighting screen (Figure 8-5).



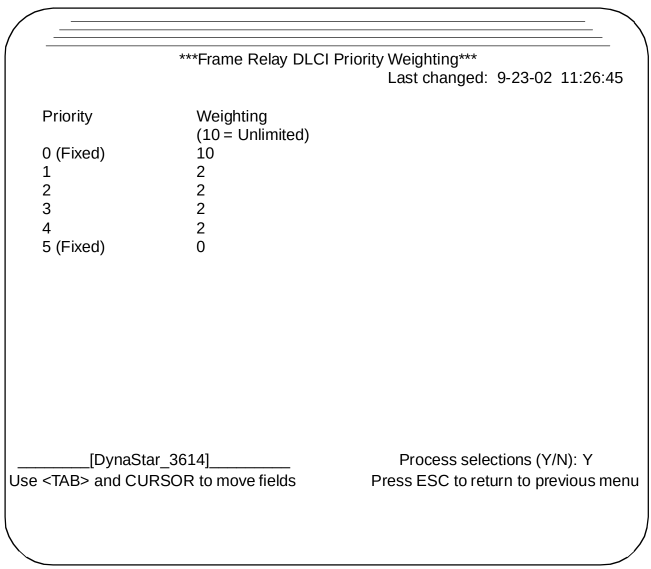


Figure 8-5 Frame Relay DLCI Priority Weighting

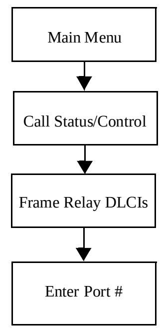
If you want priority 1 to always go before priority 2, set the weighting of priority 1 to 10. If 9 priority 1 frames are to go before each priority 2 frame, set the weighting to 9, and so

on. Be careful not to starve applications at times of heavy demand. In some cases, it may be better to set the CIR to limit lower priority traffic rather than blocking it completely.

FRAME RELAY DLCI STATUS SCREEN. You can check the bandwidth that is being used by each DLCI from the DLCI Status screen (Figure 8-6).

```
                        ***Frame Relay DLCI Status***

Source        Dest          Type          State        Packets        Rate (Kbits/sec)
Port   DLCI   Port   DLCI                              Source   Dest  Source   Dest
101    400                  RFC 1490      ACTIVE       2384     2385  3.4      23.1
102           101    100    PAD-FR        ACTIVE       0        0     0.0      0.0
102           101    200    PAD-FR        ACTIVE       0        0     0.0      0.0
102           101    300    PAD-FR        ACTIVE       0        0     0.0      0.0
108           101    500    TRANSPARACTIVE             47       153   0.0      0.0



 _________[DynaStar_3614]_________
Press <RET> for update                              Press UP/DOWN to scroll
Press <CTRL-D> to clear statistics           Press ESC to return to previous menu
```

Figure 8-6 Frame Relay DLCI Status Screen



SYSTEM PARAMETERS

Table 8-4 describes the system parameters that are used for frame relay. The values for these parameters are set by *DYNASTAR* and are not configurable by the user.

Table 8-4 Frame Relay System Parameters

Parameter	Description	Fixed Value
N391	Full Status Polling Cycles. The user requests a Full Status Report every N391 polling cycles. A polling cycle is a Status Enquiry and Status message exchange.	6

Table 8-4 Frame Relay System Parameters (cont.)

Parameter	Description	Fixed Value
N392	Error Threshold. The number of errors during N393 monitored events that cause the channel/user device to be declared inactive. The user can also use this number as the number of errors during N393 monitored events that cause the network to be declared inactive.	3
N393	Monitored Events Count. From the network's perspective, a monitored event is the receipt of a Status Enquiry message or the expiration of timer T392. From the user's perspective, a monitored event is the transmission of a Status Enquiry message. This parameter specifies the size of the sliding window that is used by the network (or user) to determine whether a channel or user device is active.	4
T391	Link Integrity Verification Timer. Indicates how frequently the user should initiate a Status Enquiry message.	10 seconds
T392	Polling Verification Timer. Indicates the length of time the network should wait between Status Enquiry messages. If no Status Enquiry message is received within T392 seconds, the network records an error.	15 seconds

■ FRAME RELAY ACCESS DEVICE (FRAD)

The *DYNASTAR* can function as a Frame Relay Access Device (FRAD) and transport asynchronous data streams over a Frame Relay network connection. There are several methods for doing this; each method has its own benefits, depending on the application that is running end-to-end.

The first method is simply to package the asynchronous data streams directly into a Frame Relay payload using X.3 protocol. No other protocol is involved. A two-byte frame relay header is pre-pended to the data packets, and they are dispatched. This method uses the least overhead and is therefore very efficient and simple to set up. However, it lacks any method for automatic data recovery in case of errors. This method is usually used in a permanent circuit configuration that does not easily allow alternate routing if the frame relay circuit fails. With this method, the application must compensate for errors in the data, missing packets, and non-responsive devices. The configuration for this method is described in Chapter 19, *Utility Features*.

The second method is to adopt the full asynchronous PAD functions in acordance with X.3, X.28, and X.29 CCITT standards and package data streams into an X.25 format that can then be transported over frame relay using Annex F or G tunnels. This adds an overhead of 5 bytes to the total payload but will provide automatic data recovery for corrupted data. It can also be set up to automatically reroute around path failures so that the application does not need any error recovery features. This X.25-FRAD method and its configuration is described later in this chapter.

This third method takes the asynchronous data stream and packages it into a TCP/IP formatted frame using a traditional terminal server function. The frame is then forwarded over the frame relay network using the RFC 1490 standard. This provides all the error recovery features of the X.25/FRAD method, it can be automatically routed around failed circuits, and it is directly compatible with many corporate networks. The only drawback is that the payload overhead is 50 bytes, which can be excessive over low-speed WAN connections. Therefore, prioritizing this information over other IP traffic may present a problem.

■ INTRODUCTION TO X.25 OVER FRAME RELAY

The X.25-FRAD (Frame Assembler-Disassembler) support available on the *DYNASTAR* allows the *DYNASTAR* to exchange X.25 packet data over Frame Relay networks. It also allows the *DYNASTAR* to interoperate with other systems that adopt the same encapsulation technique. This implementation, called X.25-FRAD, is based on the RFC 1490 specification for encapsulating data traffic over Frame Relay networks. By encapsulating X.25 LAPB frames directly inside the payload field of a Q.922 frame, the *DYNASTAR* can transport X.25 layer two and three protocol procedures over frame relay logical channels instead of over regular dedicated X.25 ports.

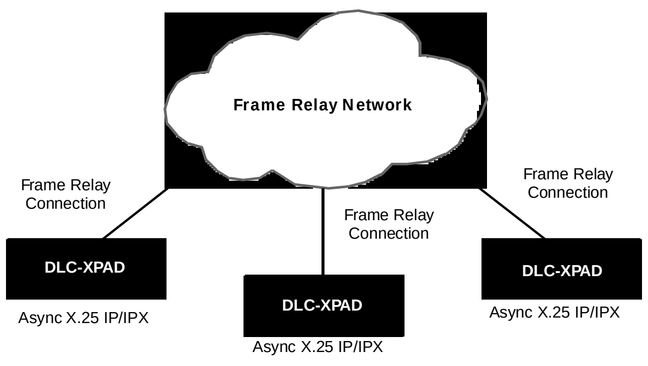


Figure 8-7 X.25 Traffic over a Frame Relay Network

Interconnected X.25-FRADs provide end-to-end conversion and encapsulation services, establishing reliable LAPB connections over Frame Relay permanent virtual circuits. This allows the *DYNASTAR* applications, such as the X.3/X.28/X.29 PAD, to forward X.25 traffic over a Frame Relay network interface instead of a traditional X.25 connection. As an X.25 concentrator, the X.25-FRAD can also be used to multiplex traffic of several X.25 lines onto one or more frame relay network connections.

The *DYNASTAR* also supports two other methods for implementing the FRAD. These are described in Chapter 19, *Utility Features*.

ENCAPSULATION OF X.25 OVER FRAME RELAY

The X.25-FRAD encapsulation technique is based on RFC 1490. LAPB frames transmitted over the frame relay network are encapsulated in a Q.922 frame. Because RFC 1490 does not specify a Network Level Protocol ID (NLPID) or an IEEE Subnetwork Access Protocol (SNAP) value for X.25 data, the X.25-FRAD uses the NLPID value of X‘08’ to imply encoding according to rules defined in ITU-T Q.933. According to this recommendation, the four octets following this NLPID identify the layer 2 and layer 3 protocol of the imbedded protocol data unit. The X.25-FRAD sets the two-octet layer 2 protocol field to 0600 to indicate an X.25 link layer and the two-octet layer 3 protocol field to 0600 to indicate an X.25 packet layer.

VIRTUAL X.25 PORT MAPPING ONTO FRAME RELAY

To forward X.25 traffic over the *DYNASTAR* frame relay ports, the X.25-FRAD implements a scheme in which users configure a new type of port called a Virtual X.25 Port (VXP). Up to 32 VXPs are supported. In addition, *DYNASTAR* users can continue to define traditional ports to support different types of interfaces such as X.25 line,PAD, PPP, and Frame Relay.

While the physical behavior of a regular port is governed by its assigned type of interface, a VXP has no external physical behavior and is not associated with an external connector. The VXP can be used only to carry X.25 traffic, but, unlike a regular X.25 port, it only supports layers 2 and 3 of the X.25 protocol. A VXP can be configured to use any of the *DYNASTAR*’s frame relay ports as its physical port.

The scheme is based on associating a VXP with a unique frame relay PVC. This is done by first assigning a frame relay port to a VXP and then assigning to it the Data Link

Connection Identifier (DLCI) of the PVC earmarked for X.25 encapsulated traffic. A frame relay PVC can be used by only one VXP. However, because a frame relay port can support several PVCs, several VXPs can be mapped to a single frame relay port.

Because a VXP supports all but the physical attributes of a physical X.25 port, it allows up to 64 SVCs to be established over a single frame relay PVC. Additional SVCs can be routed over a frame relay port by mapping several VXPs onto the same frame relay port.

The mapping scheme allows outgoing X.25 traffic through a VXP to be forwarded over frame relay ports, and it allows incoming X.25 traffic from frame relay ports to be internally routed to the *DYNASTAR* applications as if it were received on regular X.25 ports.

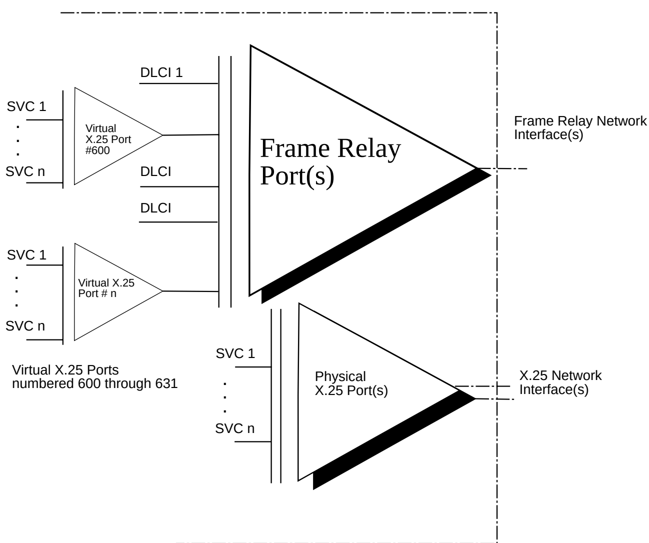


Figure 8-8 Relationship between the Frame Relay Network and the X.25 Ports

X.25 SESSIONS OVER A FRAME RELAY PVC

When the *DYNASTAR* is turned on, network paired X.25-FRADs automatically attempt to establish the X.25 link level

(LAPB) for each VXP enabled on the PVC(s) that are established between them. Once LAPB is established, traditional X.25 call establishment, data transfer, and clearing procedures can take place as they would over regular X.25 circuits. Calls and data traffic from X.25 network-bound applications at either end of the PVC can be initiated and are transferred transparently across the proxy frame relay network. Consequently, a failure of the underlying frame relay PVC or frame loss due to network congestion will trigger standard X.25 link and packet level recovery procedures as if the failure occurred on a regular X.25 link.

Frame relay networks typically support larger frames than their X.25 counterparts, and their tariff structure is traffic sensitive. The user should consider adjusting the X.25 link and packet level parameters to optimize the use of the frame relay network.

■ Configuring X.25-FRAD Parameters

Before you can specify VXP parameters, you must configure the X.25 FRAD to support one or more frame relay ports to interface to the frame relay network.You also need to define the DLCIs for each of the ports' PVCs, which will be used to transport the VXP traffic. The order of the steps for configuring the FRAD is:

- Frame relay parameters
    - Network ports
    - DLCIs
- Virtual X.25 ports (VXPs)
- X.121 addresses and switching table

Configure Frame Relay Parameters

The frame relay configuration consists of defining the network ports and the DLCIs.

DEFINE NETWORK PORTS. You must define one or more frame relay ports to enable the operation of the X.25-FRAD.

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands Menu (Figure 3-11) is displayed.

2. Select **Port**.

✓ The Configure Ports menu, containing a list of ports, is displayed.

3. Select a port that will use the frame relay protocol.

4. On the screen that is displayed, select **Frame Relay** as the port type.

✓ A screen similar to the one in Figure 8-1 is displayed.

5. Configure the parameters as required for your network. Detailed information about the parameters can be found in Table 8-2.

6. When your entries are complete, enter **Y <return>** in the field **Process selections**.

✓ You return to the Configure Port menu. The message *Changes made for Port n* appears near the bottom of the screen if you have made changes.

7. If you have other frame relay ports to configure, repeat steps 2 through 6.

8. When you have configured all the frame relay ports, continue with your configuration as explained in the next section, *Define DLCIs*.

DEFINE DLCIS. Once the frame relay ports have been defined, you must define the DLCIs that you plan to use for forwarding the encapsulated VXP X.25 traffic.

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. Select **Frame Relay**.

✓ The Frame Relay Parameters menu (Figure 8-3) is displayed.

3. Select **Frame Relay DLCIs**.

✓ The Frame Relay DLCI Configuration Table (Figure 8-4) is displayed.

4. Configure the parameters as required for your network. These parameters are described in Table 8-2.

NOTE: Make a note of the DLCIs that you configure for VXP traffic, since you will be required to enter their values later when you are configuring the VXP profiles.

CONFIGURE VIRTUAL X.25 PORTS

Once you have configured the frame relay ports and the DLCIs that you will use for VXP traffic, you can define the virtual X.25 ports.You can define up to 32 virtual X.25 ports.

1. From the Main menu, select **Configuration**.

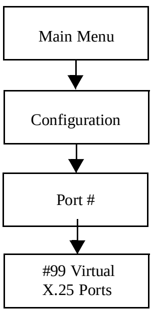
✓ The Configuration Commands menu (Figure 3-11) appears.

2. Select **Port**.

✓ The Configure Port menu, containing a list of available ports, is displayed.

3. From the Configure Port menu, select **Virtual X.25 Ports**.

✓ A screen similar to the one in Figure 8-9 is displayed, showing the 32 virtual X.25 ports that are available for routing X.25 traffic over the previously configured PVCs of the frame relay ports.

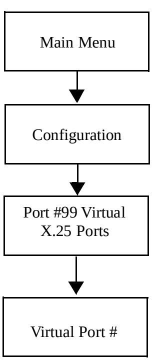



```
                         ***Virtual X.25 Ports ***

Valid port numbers (with names) are:
600: VXP London                       616: V X25 Port 616
601: VXP1 Paris                       617: V X25 Port 617
602: VXP2 Paris                       618: V X25 Port 618
603: V X25 Port 603                   619: V X25 Port 619
604: V X25 Port 604                   620: V X25 Port 620
605: V X25 Port 605                   621: V X25 Port 621
606: V X25 Port 606                   622: V X25 Port 622
607: V X25 Port 607                   623: V X25 Port 623
608: V X25 Port 608                   624: V X25 Port 624
609: V X25 Port 609                   625: V X25 Port 625
610: V X25 Port 610                   626: V X25 Port 626
611: V X25 Port 611                   627: V X25 Port 627
612: V X25 Port 612                   628: V X25 Port 628
613: V X25 Port 613                   629: V X25 Port 629
614: V X25 Port 614                   630: V X25 Port 630
615: V X25 Port 615                   631: V X25 Port 631

                      Enter virtual X.25 port number:
 ________[DynaStar_3614]_________
Cursor UP/DOWN for more ports          Press ESC to return to previous menu
```

Figure 8-9 List of Virtual X.25 Ports

4. Select the number of the port you want to define.

✓ A screen similar to the one in Figure 8-10 is displayed.




```
                    *** Virtual X.25 Port Configuration ***
Port: 601                                     Last changed:   5-4-02 11:26:45

|- Press <RET> to toggle values -||-- Type in values.  Max chars shown in () --|
                                Port name:            VXP2 Paris          (14)
                                X.121 Address:             300        (15 BCD)


LAPB extended:          N        K   LAPB window size:        7         (fixed)
X.25 mode:              DTE      T1  Acknowledgement timer:   3    (1-255 sec)
Calling address mod:    NONE     T3  Idle Timer:              30   (0-255 sec)
Max Window size:        7        N2  Retransmission count:    20       (1-255)
Max Packet size:        1024     N1  Max frame size:          8248 bits
Packet/Window Neg:      Y
Require CUG:            N
Require NUI:            N
Req Reverse Charging:   N        LCN Partition     Base LCN     Number of VCs
                                                  (1-4095)
Traffic types permitted on line:   One-way in:       1             0
  IP Routing          Y            Two-way:          1             64
  IPX Routing         N            One-way out:      4095          0
  Ethernet Bridging   N

 ________[DynaStar_3614]_________                  Process selections (Y/N): Y
Use TAB & CURSOR keys to move among fields.   Press ESC to abort command & exit.
```

Figure 8-10 Virtual X.25 Port Configuration Screen

5. Complete the parameters as required for your network. (See Chapter 6, *The X.25 Application*, for an explanation of general X.25 parameters.)
6. When you have completed your entries, enter **Y <return>** in the **Process selections** field.

✓ You return to the Virtual X.25 Ports screen (Figure 8-9). The message *Changes made for Port n* appears near the bottom of the screen if you have made any changes.

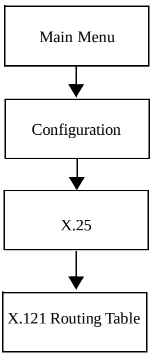
7. Repeat steps 4 through 6 for any additional ports you wish to define.
8. When you have defined all the virtual ports, continue your configuration as explained in the next section, *Configure X.121 Addresses and Switching Table*.

Configure X.121 Addresses and Switching Table

The X.121 addresses and the switching table are used to route calls from *DynaStar* applications to outbound X.25 lines. It is not used to route incoming calls from the X.25 network. Virtual X.25 ports use the same X.121 and switching mechanisms as standard X.25 ports. The X.25-FRAD does not require special parameters nor does it use special configuration screens.

For example, to route incoming calls from X.25, other VXPs, or PAD ports to outbound VXPs, you use the X.25 Concentrator Routing Table (Figure 8-11) to associate X.121 called addresses with selected VXPs. The X.25-FRAD presents you with the option of selecting VXPs (in addition to regular ports) when you toggle the port values in the Port column of the screen.

Please refer to Chapter 6, *The X.25 Application*, for more information on the fields in this screen and the routing capabilities of the unit.




```
                    *** X.25 Concentrator Routing Table ***
                                          Last changed:   4-23-02 11:26:45

 X.121 address      Shared  |-- Use <RET> to toggle values --|X.32 dial line phone number
 (1-15 BCD,D & X) Scheme Port    Priority       Dial speed              (max 19 characters)
1: 13000                     13          1
2: 31012345678               600         1
3: 31012345679               601         1
4: 31012345680               602         1
5: 31012345681               603         1
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:
  _________[DynaStar_3614]__________                     Process Routing tables(Y/N): Y
Search for X.121 Address:                                 Select Share Scheme:
To change or add entry, enter new value                   Use <CTRL-D> to delete entry
Use TAB & CURSOR keys to move among fields.   Press ESC to abort command & exit.
```

Figure 8-11   X.25 Concentrator Routing Table

In addition to the X.25 Concentrator Routing Table, there are several other configuration screens that let you route LAN traffic over X.25 by assigning IP and IPX addresses to ports. The X.25-FRAD allows you to do the same for the virtual X.25 ports. There are no special parameters or procedures required to route LAN traffic over a VXP. You simply configure the VXP as you would a standard X.25 port.

> **NOTE:** Although it is possible to forward LAN traffic over a frame relay network via a VXP, it is more efficient to route LAN traffic directly over the frame relay interface.

■ FRAME RELAY BACKUP VIA ISDN

The *DYNASTAR* can back up a frame relay DLCI over a secondary frame relay DLCI via ISDN. Frame relay backups over ISDN comply with ANSI recommendation T1.617 and ITU-T recommendation Q.933.

The LMI function detects when the primary DLCI has been down for a critical amount of time and activates the secondary DLCI. Traffic is then automatically rerouted over the secondary DLCI. When the primary DLCI returns to an active state, the LMI function again reroutes the traffic over the primary and disconnects the secondary DLCI.

NOTE: If the *DYNASTAR* receives a call for the port configured as the backup port at any time, the primary DLCI will immediately be replaced by the secondary DLCI.

CONFIGURING A BACKUP ROUTE FOR A DLCI

Once frame relay ports and DLCIs are configured as described earlier in this chapter, you can define backup connections as described in the following procedure.

NOTE: To enable frame relay backups, be sure to select **LMI** in the DLCI management field on the Frame Relay Port Configuration menu (Figure 8-1), described in the section *Frame Relay Port Configuration*, earlier in the chapter.

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands screen (Figure 3-11) is displayed.

2. Select **Frame Relay**.

✓ The Frame Relay Parameters screen (Figure 8-3) is displayed.

3. Select **Frame Relay Backups/Properties**.

✓ The Frame Relay Backups and Connection Properties screen (Figure 8-12) is displayed.

4. Enter the primary port number and the DLCI to be backed up.

   NOTE: The Sub-DLCI parameter is reserved for future implementation.

5. In the **Backup Type** column, select **FR** (Frame Relay) or **ISDN** to specify what type of backup connection will be used for this DLCI.

6. In the next two columns, specify the outgoing port number and DLCI for the backup connection.

7. If you have specified an ISDN connection, enter the telephone number of the remote *DYNASTAR* to which frame relay traffic will be routed when this DLCI is down.

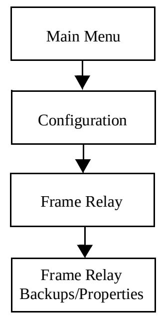
   NOTE: The telephone number must be one of those configured on the Incoming ISDN Telephone Numbers menu of the remote *DYNASTAR*, and it must be assigned to one of the remote *DYNASTAR*'s ISDN ports configured for frame relay traffic.

8. Repeat the previous steps to configure backup for any additional DLCIs.

9. When you have completed your entries, enter **Y** in the **Process Table selections** field and press **<return>**.

✓ Backup of the specified DLCIs is enabled for this *DYNASTAR*.

   NOTE: The backup process will not work unless the remote *DYNASTAR* also is configured for backup.




```
                    ***Frame Relay Backups & Connection Properties***
                                                  Last changed:  4-5-02  11:26:45

    Primary                       Backup
    Port   DLCI  Sub-DLCI  Type  Port   DLCI  Sub-DLCI        Telephone Number
1:  101    15              ISDN  101    21                    2223456
2:
3:
4:
5:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:
16:
  ________[DynaStar_3614]_________            Process Table selections (Y/N): Y
 In Type field, use UP/DOWN to scroll and LEFT to process selections.
 To change or add entry, enter new value.                Use <CTRL-D> to delete entry.
 Use TAB & CURSOR keys to move among fields.    Press ESC to abort command & exit.
```

Figure 8-12 Frame Relay Backup and Connection Properties Screen

When you configure a backup connection for a local Frame Relay DLCI, you must also configure a mirror backup connection for the remote DLCI. For example, Figure 8-13 shows a primary connection through a Frame Relay network with a secondary backup over ISDN. Frame relay backup is configured for both *DYNASTAR A* and *DYNASTAR B* as described in the tables that follow.

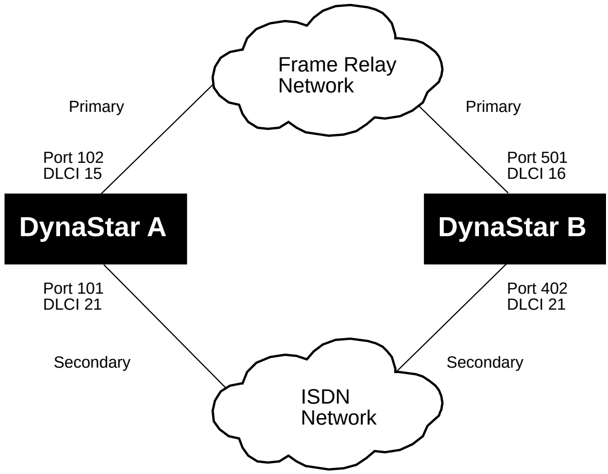


Figure 8-13 Frame Relay Connection with Backup Via ISDN

DynaStar A

Frame Relay Backups & Connection Properties Menu

Primary	DLCI	Backup	Port	DLCI	Telephone Number
102	15	ISDN	101	21	2223456

Port 101 Configuration Menu

ISDN Telephone Number: 2227890

ISDN Incoming Telephone Number Menu for Slot 1 (Trunk 100)

Port	Telephone #	Protocol	SPID
01	2227890	Frame Relay	N/A

Frame Relay Backups & Connection Properties Menu

Primary	DLCI	Backup	Port	DLCI	Telephone Number
501	16	ISDN	402	21	2227890

Port 402 Configuration Menu

ISDN Telephone Number: 2223456

ISDN Incoming Telephone Number Menu for Slot 4 (Trunk 400)

Port	Telephone #	Protocol	SPID
02	2223456	Frame Relay	N/A

ISDN CONFIGURATION

■ ISDN CAPABILITIES

The *DYNASTAR 100i* provides built-in ISDN capabilities. Several daughterboards provide ISDN capabilities for the other *DYNASTAR* models.

The BRI interface provides a 2B+D (two B channels plus one D channel) connection; the PRI interface provides a DS1 connection at 1.544 Kbps for T1 or 2.048 Kbps for E1. For additional information on these interface cards, see the section *Optional Configurations* in Chapter 1, *Introduction*.

This chapter describes the configuration of all ISDN interfaces available on the *DYNASTAR*. For information on monitoring an ISDN interface, see Chapter 19, *Monitoring and Statistics*.

THE BASIC RATE INTERFACE

The ISDN Basic Rate Interface, or BRI, consists of three virtual channels: two 64 kbps B-channels and one 16 kbps D-channel (for signaling and X.25). A dual BRI—with two sets of 2B+D channels—is available as an optional interface card.

T1/E1/PRI DAUGHTERBOARD

The T1/E1/PRI daughterboards enable your *DYNASTAR* to connect to 1.544 Mbps T1 service and/or to 2.048 Mbps E1 service. You can configure the PRI version of this board to provide channelized T1/E1/PRI service or to provide ISDN PRI (Primary Rate Interface) service, with n x 64 or (in some cases for T1) n x 56 kbps channels.

NOTE: Two versions of the ISDN daughterboard are available. One version can provide both PRI and channelized service. The other version provides only channelized service. If you have difficulty establishing a PRI circuit, be sure you have a daughterboard with full capability in the associated slot. The heading on the Trunk Parameters screen identifies the card type as either **PRI Capable** or **Channelized Only**. The two boards are also distinguishable by part number.

T1/E1/PRI Trunk and Channel Numbering.

Each T1/E1/PRI board supports two trunks. The first trunk is numbered x00 and the second trunk is numbered x50, with *x* representing the slot number (1, 2, 3, 4, or 5 for the *DynaStar 500*). For example, a T1 board in slot 3 of the *DynaStar 500* has two trunks, numbered 300 and 350.

Each T1 trunk can support a maximum of 24 channels, numbered x01-x24 or x51-x74 (for example, 301-324 or 351-374). Each E1 trunk has a maximum of 31 channels, numbered x01-x31 or x51-x81. The *DynaStar* treats these channels as if they were synchronous physical ports.

Operation of the LEDs for the ISDN function is explained in Chapter 2, *DynaStar Installation*.

■ ISDN BRI and PRI Configuration Overview

ISDN configurations are associated with telephone numbers. Because of this, if your network requires different types of physical line configurations, you must define different called numbers and assign the different configurations to them.

NOTE: By default, the PRI or BRI connection will accept any incoming number and use the PPP protocol for it. Likewise, it will place an outgoing call using any port configured for PPP protocol. This default configuration should meet the needs of most users with no further configuration required. However, if you require a specialized configuration, use the following procedure.

Figure 9-1 gives an overview of the steps involved in configuring your ISDN PRI or BRI. The left-hand column identifies the screen that you will use for each major step, the center column describes the functions that you will be performing, and the right-hand column lists any additional configuration that may be required. If additional configuration is required, you will go to another screen, not shown in this diagram.

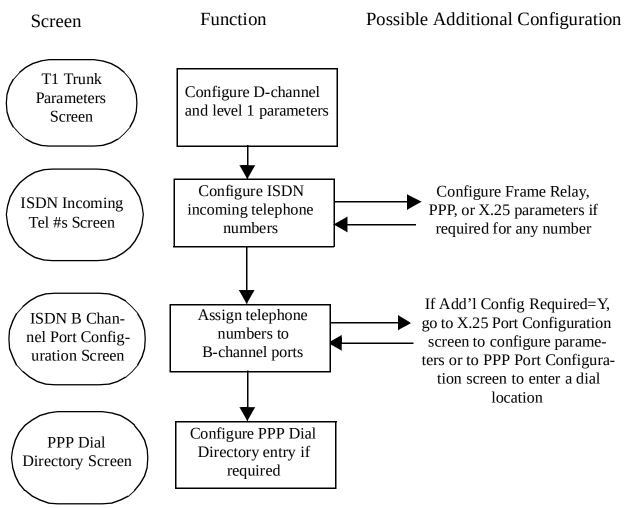


Figure 9-1 Overview of ISDN PRI and BRI Configuration

The procedures that follow provide a detailed description of the steps involved in configuring the BRI and PRI. D-channel configuration differs somewhat for BRI and PRI modules and is handled in separate sections. Although T1 PRI is often used in the example screens as the trunk type, E1 PRIs are configured much the same way. Any exceptions are noted.

NOTE: Channelized T1 and E1 configuration is covered separately later in this chapter.

Configuring the BRI D-Channel

Configure the D-channel as described in the following procedure. Table 9-1 defines parameters specific to the D-channel.

1. From the Main menu, select **Configuration**.

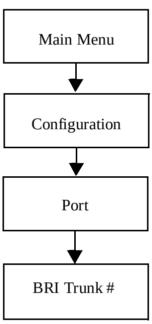
✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. Select **Port**.

✓ The Configure Port menu, containing a list of available ports, is displayed.

3. Select a BRI trunk number from the Configure Port menu.

✓ The ISDN Port Configuration menu is displayed, as shown in Figure 9-2.



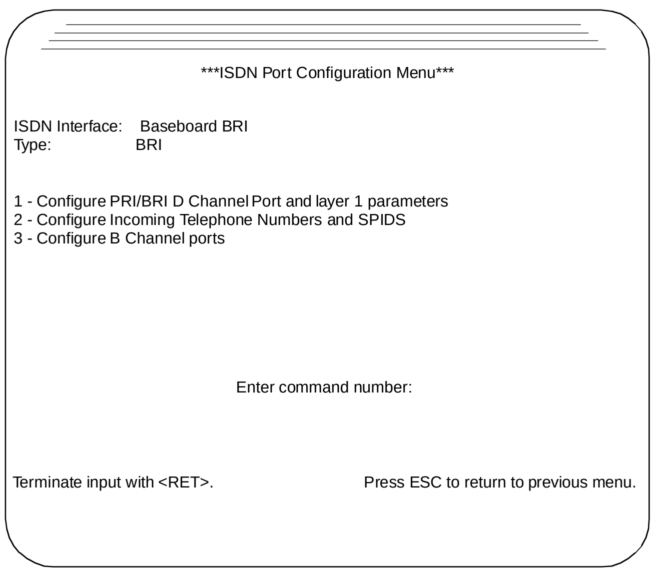


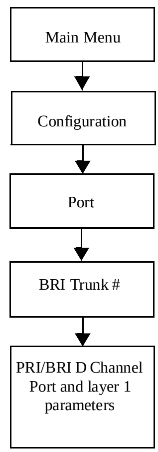
Figure 9-2 ISDN Port Configuration Menu

4. Select **Configure PRI/BRI D Channel Port and layer 1 parameters**.

✓ The ISDN D-Channel Port Configuration menu, similar to Figure 9-3, is displayed.

```
                         *** ISDN D Channel ***

   Port: 300  D Channel                       Last changed: 11/6/98  14:36:19

   |- Press <RET> to toggle values. -|  |-Type in values. Max chars shown in (). --|
   Port type:     BRI (S Interface)    Port name:    Trunk 3/1                  (14)


   Signalling type:    NI-1

   X.25 support:      N       (If yes, enter <CTRL O> to read/update X.25 parameters)
   X.25 TEI:          0       (For dynamic TEI assignment use 255)
   X.25 SAPI:        16      Choosing 0 may not work with Q.931 at the same time




                          Save changes and return to previouus menu? (Y/N):  Y
__________[DynaStar_3df2]__________
Use TAB & CURSOR keys to move among fields.   Press ESC to abort command & exit.
```

Figure 9-3 ISDN D-Channel Port Configuration Screen



5. In the **Port name** field, change the name of the channel if you wish.
6. In the **Signaling type** field, select one of the following:
   - **NI-1** (National 1, used in most of North America)
   - **NET3** (used in Europe)
   - **AT&T 5ESS** (used for some custom configurations)
   - **NDKK** (used in Japan and Europe)
7. In the **X.25 support** field, enter **Y** if the D-channel will be carrying X.25 traffic.
8. Set **X.25 TEI** to the value provided by your service provider if static TEIs are used or to 255 if dynamic TEIs are used.

   NOTE: Most service providers use dynamic TEIs.

9. If you have set **X.25 support** to **Y**, press **<Ctrl-O>**. If **X.25 support** is set to **N**, skip to step 12.

✓ The D-Channel X.25 Parameters screen (Figure 9-4) is displayed.

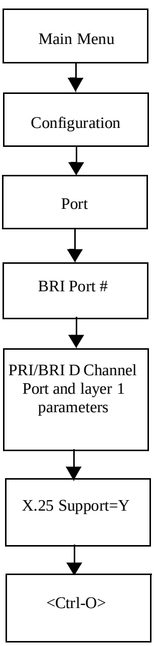
10. Adjust X.25 parameter settings as required.

NOTE: For more information on these parameters, see Chapter 6, *The X.25 Application*.

11. In the **Save changes and return to previous menu** field, enter **Y** and press **<return>**.

✓ Your changes are recorded and you return to the ISDN D-Channel Port Configuration menu. You can now use the D-channel as you would any X.25 port.

✓ You return to the ISDN D-Channel Port Configuration screen (Figure 9-3).




```
                              ***ISDN D Channel***
 Port: 300  D Channel                                Last changed: 4-23-02  11:26:45

|- Press <RET> to toggle values. -|  |-Type in values. Max chars shown in () --|
Port type:          BRI (S Interface)   Port name:   D Channel                  (14)
                                        X.121 address:                      (15 BCD)
Connection mode:          LEASED
Line speed:               9.6 kbps     Non-Zero DTE Cause:  N
Number of flags:       (0-15)    0     Allow User Data:        Y
Calling address mod:        NONE       LAPB extended:          N
Local address insert:          N       X.25 mode:             DTE
Max Window size:               7       K LAPB window size:     7              (7-127)
Max Packet size:            1024       T1 Acknowledgment timer: 3         (1-255 sec)
Packet/Window Neg:             N       T3 Idle Timer:          30         (0-255 sec)
Require CUG:                   N       N2 Retransmission count: 20            (1-255)
Require NUI:                   N       N1 Max frame size:      8248 bits
Req Reverse Charging:          N       LCN Partition      Base LCN     Number of VCs
Route inbound calls on CUD:    N                          (1-4095)
Traffic types permitted on line           Permanent:        1                  0
     IP Routing:            Y             One-way in:       1                  0
     IPX Routing:           N             Two-way:          1               4095
     Ethernet Bridging:     N             One-way out:   4095                  0

_______[DynaStar_3614]_______ Save changes and return to previous menu (Y/N): Y
 Use TAB & CURSOR keys to move among fields.    Press ESC to abort command & exit.
```

Figure 9-4 D-Channel X.25 Parameters Screen

12. Enter **Y** in the field **Save changes and return to previous menu** and press **<return>** to save and quit.

NOTE: If you exit from the ISDN D-Channel Port Configuration menu without saving, any modifications to the X.25 parameters on the underlying screen are not saved.

13. Complete your configuration by configuring the X.121 Routing Table. See the section *Configuring the X.121 Routing Table* later in this chapter.

Table 9-1 D-Channel Parameters for BRI Configuration

Parameter	**Description**	**Values**
Port type	Display only field. Cannot be changed.	D Signaling
Port name	A name to help you identify this port.	Max 14 chars Default = D-Channel
Signaling type	Signaling type compatible with that of your ISDN carrier. If you are not sure of your signaling type, here are some suggestions: In the US and Canada, try NI-1 and AT&T. Outside of North America, try NET3 and NDKK. In Japan try NDKK, NET3, and NI-1.	NI-1 Net 3 AT&T ESS NDKK Default = NI-1
X.25 support	Specifies whether the D-channel will support X.25 traffic.	Y, N Default = N
X.25 TEI	Designates the static TEI for this channel; or indicates that the TEI is dynamically assigned. The TEI (Terminal Endpoint Identifier) helps identify equipment when multiple devices are located on the bus.	1-255 (255=dynamic assignment of TEI) Default = 0

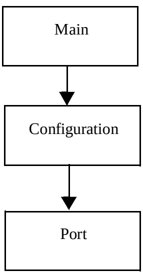
CONFIGURING THE PRI D-CHANNEL

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) appears.

2. From the Configuration menu, select **Port**.

✓ A list of available ports similar to Figure 9-5 appears.




```
                         ***Configure Port***

Valid port numbers (with names) are:
0: Ethernet
6: Console
7: Sync/Async
8: HS WAN 1
9: HS WAN 2
10: Virtual PAD
99: Virtual X.25 Ports
100: Trunk 1/1
150: Trunk 1/2


                         Enter port number:



_______[DynaStar dc000345]_______
Terminate input with <RET>.            Press ESC to return to previous menu.
```

Figure 9-5 Configure Port Menu Showing T1/E1/PRI Card

3. Select a T1/E1 trunk that you want to configure as PRI (here, 100 or 150).

✓ If this is your initial configuration of the trunk, the T1 (or E1) Trunk Parameters menu (Figure 9-16) appears. If the trunk has already been configured as PRI, the ISDN Port Configuration menu (Figure 9-6) appears.

4. If the ISDN Port Configuration menu appears, go to Step 7.

5. If the T1 or E1 Trunk Parameters screen appears, toggle the **Trunk Type** to **T1 PRI** (or **E1 PRI**). Then

move the cursor to **Process Selections**, select **Y**, and press **<return>**.

✓ A message screen appears saying that all channels will be reinitialized. Press **<return>** to continue.

> **NOTE:** If you cannot select PRI, check the heading of the Trunk Parameters screen for the type of daughterboard installed. If the heading is **Channelized Only**, this board does not support PRI.

6. You return to the Configure Port menu (Figure 9-5). Again select the PRI trunk you are configuring.

✓ The ISDN Port Configuration menu (Figure 9-6) appears.

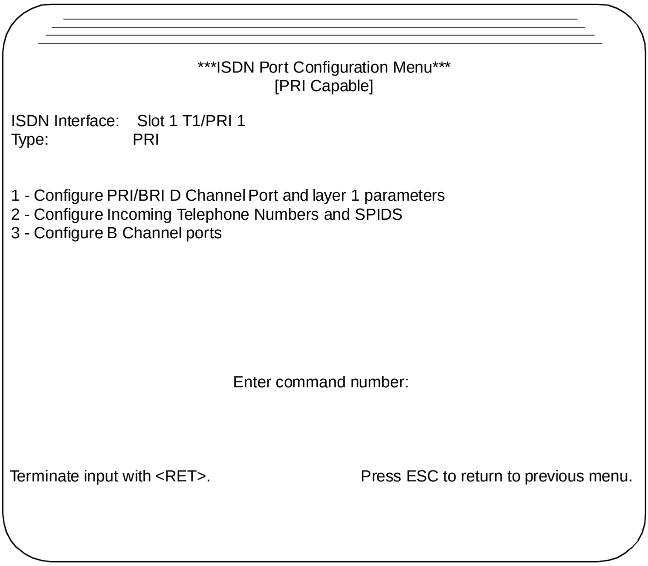
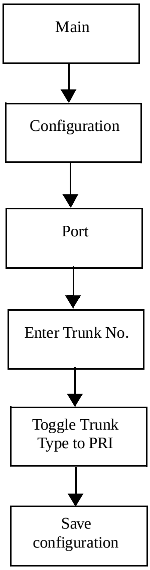
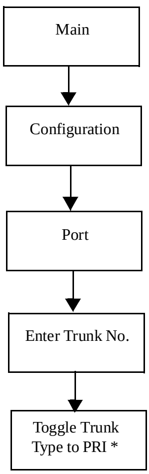


Figure 9-6 ISDN Port Configuration Menu

7. Access the T1/E1 Trunk Parameters screen by selecting **Configure PRI/BRI D Channel Port and layer 1 parameters**.

8. Retain **PRI** as **Trunk Type**.





* Or select Configure D Channel from ISDN Port Configuration menu.

✓ The T1 Trunk Parameters screen for PRI, shown in Figure 9-7, appears. This screen lets you configure the signaling for the D-channel of a PRI connection and the layer 1 T1/E1 parameters.

```
                         ***T1 Trunk Parameters***
                               [PRI Capable]
Port: 100                                   Last changed  : 4-23-02    23:45:00
Trunk Type:    T1 PRI                       Trunk Name    :   Trunk 1/1        (14)

Frame Type:        ESF                      D Channel Bandwidth:   64 Kbps
Line Coding:       B8ZS                     Yellow Alarm Mode:     FDL
CRC 6:             On                       Line Build Out:        0 to 133 ft
                                            Transmit Clk source:   Local oscill.
Signaling Type:    NI-1
Device Type:       USER




_______[DynaStar dc000345]_______               Process selections (Y/N): Y
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 9-7 T1 Trunk Parameters for PRI Board

9. Configure the parameters as required by your network. For details on parameters, see Table 9-2.

10. When you have finished configuring the parameters, enter **Y** at **Process selections** and press **<return>**.

Table 9-2 T1/E1/PRI Trunk Parameters

Parameter	Description	Values
Trunk Type	Determines how the trunk is defined: to handle fixed-configuration channelized T1/E1 traffic or PRI traffic. (PRI is discussed in the section *ISDN PRI Configuration*.) NOTE: Depending on the type of board you have installed, PRI may not be available. See the section *T1/E1/PRI Daughterboard* for more information.	T1 channelized E1 channelized (defaults) PRI
Trunk Name	A name to help you identify this trunk.	Max 14 chars The default name is Trunk x/1 or x/2, where x = slot # and 1 or 2 = trunk #
Frame Type	The type of framing used on the trunk. Note: For an E1 PRI configuration, the frame type is always FAS.	For T1: ESF (default) D4 For E1: FAS (default) CAS
Line Coding	The type of coding used on the line: Alternate Mark Inversion (AMI), in which each 1 bit changes polarity from the preceding 1 bit, or Bipolar with 8 Zero Substitution (B8ZS), which allows all 64 kbps to be used in data transmission. For E1 lines: AMI or High Density Bipolar 3-zeros (HDB3), which replaces four zeros with a bipolar violation.	For T1: B8ZS (default) AMI For E1: HDB3 (default) AMI
CRC 6 (T1) CRC 4 (E1)	When set to On, a cyclic redundancy check is performed and included in the framing algorithm. Note: If Frame Type = D4 (T1 only), this field is not used.	On (default) Off

Table 9-2 T1/E1/PRI Trunk Parameters (cont.)

Parameter	**Description**	**Values**
Signaling Type (PRI only)	Set signaling to match that used by your carrier.	NI-1 (mainly used in North America) NET5 (used in Europe) NDKK (Japan and Europe) AT&T 5ESS (for custom configurations)
Device Type	Indicates what type of device is connected to your port.	User Network
Time Slot Bandwidth (T1 channelized only) D Channel Bandwidth (T1 PRI only)	Indicates if the entire 64 kbps per time slot will be used or only 56 kbps. The 56 kbps and 64 kbps selections set bandwidth on every timeslot. When the option Either is selected, each timeslot can be programmed individually to use 56 kbps or 64 kbps. This parameter is not shown for E1 PRI, as the D-channel bandwidth is always 64 kbps.	56 kbps 64 kbps (default) Either
Yellow Alarm Mode (T1 only)	Type of alarm signaling. This parameter is set to FDL (facility data link) when Frame Type = ESF and cannot be changed. If Frame Type = D4, the options are bit 2 (all time slots) or Fs bit 12 (bit 12 of frame).	FDL (set if Frame Type= ESF) bit 2 (default if Frame Type=D4) Fs bit 12
Line Build Out (T1 only)	Set this parameter to equal the length of the wire from your facility to the location of the first repeater. If you are connecting to a CSU, set the appropriate attenuation.	0 to 133 feet 133 to 266 feet 266 to 399 feet 399 to 533 feet 533 to 655 feet -7.5 dB -15 dB -22.5 dB

Table 9-2 T1/E1/PRI Trunk Parameters (cont.)

Parameter	Description	Values
Interface type (E1 only)	Set this parameter to agree with the interface module you have installed. Use the option 75 Ohm COAX if the module has BNC connectors. Use the option 120 Ohm Balanced if the module has RJ-45 connectors.	75 Ohm COAX 120 Ohm Balanced
Transmit clk source	Indicates the clock source. If the wrong value is selected here, it can affect the number of slips as seen on the statistics screen. You normally select the value Receive clock for the trunk you are configuring.	Local oscill (default) Trunk 1 Rx clk Trunk 2 Rx clk

Configuring ISDN Incoming Calls

1. Be sure you have configured the trunk type as PRI or BRI (as described in the previous sections on configuring the D-Channel).

2. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu is displayed.

3. Select **Port**.

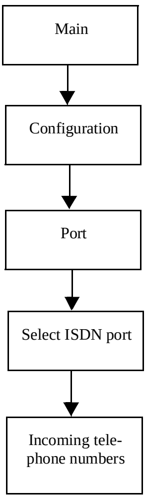
✓ The Configure Port menu is displayed.

4. Enter the ISDN Trunk number.

✓ The ISDN Port Configuration menu (Figure 9-6) is displayed.

NOTE: If you are configuring a BRI trunk, you can only enter two telephone numbers on this menu. For a PRI trunk, you can enter a maximum of five telephone numbers.

5. Select **Configure Incoming Telephone Numbers and SPIDs**.



✓ The ISDN Incoming Telephone Numbers screen, shown in Figure 9-8, appears. Initially, the top telephone number field contains the word DEFAULT. This allows a call from any phone number to be accepted using the PPP protocol.

```
                         ***ISDN Incoming Telephone Numbers***
ISDN Interface: Slot 1 TI/PRI1                           Last changed: 4-23-02 13:57:46

     Telephone # (16)    Protocol     Class      SPID (BRI NI-1 & AT&T only) (30)
     ----------------    ----------   ------     -----------------------------------------
01   DEFAULT             PPP          NONE
02
03
04
05

_______[DynaStar dc000345]_______            Process Incoming Numbers (Y/N): Y
To DELETE an entry use <CTRL-D>.To change the protocol or to configure protocol
options cursor to the desired entry and enter <CTRL-O>. To view the modem options
cursor to the desired entry and enter <CTRL-B>.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 9-8 ISDN Incoming Telephone Numbers Screen

6. In the **Telephone #** field, enter the incoming phone numbers that you expect to receive. (Hyphens and parentheses can be used for readability; they will be ignored.)

NOTE: You can delete the DEFAULT entry, but if you do and a call is received for a telephone number that is not otherwise defined on this screen, the call is not answered.

7. If you need to configure PPP or X.25 parameters for a particular phone number, first enter the phone number and then enter **<CTRL-O>** on the line where you need to set parameters.

✓ The PPP Synchronous Port Configuration screen appears.

8. Set the parameters as required for PPP, or toggle the **Port Type** field to select **X.25 line** or **Frame Relay** and then set the parameters for the selected protocol type. (See Chapter 6 for more information on X.25 and Chapter 8 for more information on frame relay.)

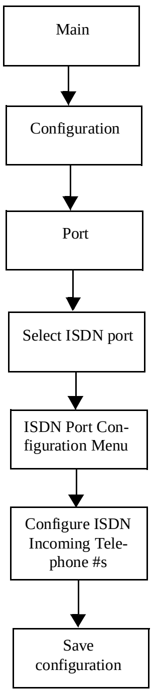
9. Enter **Y** at the **Process selections** prompt and press **<return>**.

✓ You return to the ISDN Incoming Telephone Numbers screen (Figure 9-8).

10. Complete your configuration.

NOTE: The modem classes column lets you select or define the type of modem being used for this call. You can access this information by entering <CTRL-B> or by selecting Modem Classes from the Configuration menu. The SPID field applies only to configurations using an NI-1 or AT&T interface.

11. When you have completed the configuration of all the phone numbers, enter **Y** at **Process Incoming Numbers** and press **<return>**.



✓ The message screen shown in Figure 9-9 appears to remind you to assign any newly defined telephone numbers to a B-channel.

```
***MESSAGE SCREEN***

A new telephone entry has been defined. It needs to be assigned
to a B channel port before it can be used.

Control will pass to the B Channel port configuration screen so
 that the assignment can be made.

PRESS ESC OR ENTER TO CONTINUE.
```

Figure 9-9 B-Channel Configuration Reminder Screen

12. Press **<return>** to complete the configuration.

✓ The ISDN B Channel Port Configuration screen, as shown in Figure 9-10, appears. This screen allows you to configure 30 ports (channels) for E1 PRI, 23 for T1 PRI, or 2 ports for BRI. The screen scrolls to show all entries. The default configuration allows all ports to accept and place calls using any telephone number and the PPP protocol. The next section explains how to configure this screen.

```
                    ***ISDN B Channel Port Configuration***
ISDN Interface: Slot 1 PRI 1                        Last changed: 4-23-02  13:35:44

  Port   Use       Inbound Tel #    Protocol   ML     Full Time    Config Required
  ------ ---------- ---------------- -------   -        -               -
  101    IN/OUT    DEFAULT          PPP        Y
  102    IN/OUT    DEFAULT          PPP        Y
  103    IN/OUT    DEFAULT          PPP        Y
  104    IN/OUT    DEFAULT          PPP        Y
  105    IN/OUT    DEFAULT          PPP        Y
  106    IN/OUT    DEFAULT          PPP        Y
  107    IN/OUT    DEFAULT          PPP        Y
  108    IN/OUT    DEFAULT          PPP        Y
  109    IN/OUT    DEFAULT          PPP        Y
  110    IN/OUT    DEFAULT          PPP        Y
  111    IN/OUT    DEFAULT          PPP        Y
  112    IN/OUT    DEFAULT          PPP        Y
  113    IN/OUT    DEFAULT          PPP        Y
  114    IN/OUT    DEFAULT          PPP        Y
  115    IN/OUT    DEFAULT          PPP        Y

_______[DynaStar dc000345]_______   Process B channel port configuration (Y/N): Y
To DELETE an entry use <CTRL-D>.         To configure port options use <CTRL> O.

Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 9-10 B Channel Port Configuration Screen

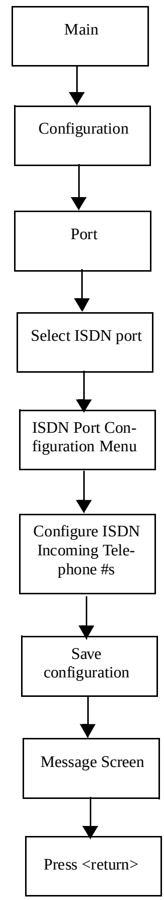
NOTE: For information on how directory numbers are checked and used, see the section *Directory Number Matching* later in this chapter.

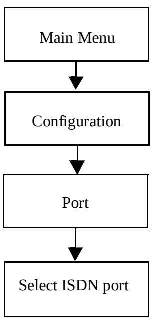
CONFIGURING THE B-CHANNELS

Configure the B-channels as described below. Table 9-2 includes the parameters that can be defined for a PRI B-channel. Table 9-3 defines the PPP options that can be configured for the B-Channels.

1. From the Main menu, select **Configuration**.
2. The Configuration Commands menu is displayed.
3. Select **Port**.
4. Select the trunk type.

✓ The ISDN Port Configuration menu (Figure 9-11) is displayed. The type of interface you selected is shown near the top of the menu.






```
                    ***ISDN Port Configuration Menu***
                              [PRI Capable]

ISDN Interface:   Baseboard BRI
Type:             BRI


1 - Configure PRI/BRI D Channel Port and layer 1 parameters
2 - Configure Incoming Telephone Numbers and SPIDS
3 - Configure B Channel ports



                        Enter command number:



Terminate input with <RET>.          Press ESC to return to previous menu.
```

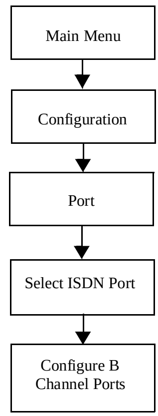
Figure 9-11   The ISDN Port Configuration Menu

5. Select **Configure B Channel ports**.

✓ The ISDN B Channel Port Configuration menu (Figure 9-12) is displayed.

```
                    ***ISDN B Channel Port Configuration***
ISDN Interface: Baseboard BRI                     Last changed: 3-15-02 13:35:44

   Port Use       Inbound Tel #  Protocol  Classes  ML    Full Time  Config Required
   ------ ----------  -----------------  -------  ----------  -     --
  101   IN/OUT   DEFAULT       PPP       None     Y
  102   IN/OUT   DEFAULT       PPP       None     Y



_______[DynaStar dc000345]_______      Process B channel port configuration (Y/N): Y
To DELETE an entry use <CTRL-D>.To configure port options use <CTRL> O.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 9-12 B Channel Port Configuration Screen for BRI



6. Select **IN/OUT**, **IN**, or **OUT** in the **Use** column to indicate whether the channel will be used for incoming calls, outgoing calls, or both.

✓ The screen repaints depending on your selection.

7. If the channel handles inbound traffic, toggle the **Inbound Tel #** field to the incoming telephone number that will be directed to this channel port.

NOTE: **Inbound Tel #** is blank if **Use** is set to **Out**; otherwise, it toggles between **DEFAULT** and the values entered in the ISDN Incoming Telephone Numbers screen (Figure 9-8).

8. If you have selected **OUT** as the **USE** type, select **PPP**, **Frame Relay**, or **X.25** in the **Protocol** column. (If **IN** or **IN/OUT** appears in the **USE** field, the **Protocol** field is automatically set to the protocol that was defined for the given inbound telephone number on the ISDN Incoming Telephone Numbers screen.)

NOTE: If you are using the B-channels for IP routing or IPX routing or bridging, the channels should be configured for PPP protocol.

9. Toggle the **ML** field to indicate whether the port can join an active PPP multilink bundle.

NOTE: Each multilink connection requires two ports for increased bandwidth. The multilink field is used to restrict the number of B-channels that can be bundled, so that a certain number of connections can be made. For example, if only 3 ports are set to **ML=Y**, then the *DYNASTAR* will be able to establish 20 distinct connections. If **Use=In** and **Protocol=X.25**, or if **Full Time=Y**, this field is not applicable.

NOTE: It is recommended that ports with multilink enabled be configured at the end of the ports list.

10. Select **Y** in the **Full Time** column if this is a dedicated outgoing line (on which the call will not normally be disconnected). This option is valid only when **Use** is set to **Out**. When **Full Time** is set to **Y**, the call is connected automatically during startup. Select **N** if the outgoing line is an on-demand line.

NOTE: For PPP, the full time setting can be used for IP and IPX routing and bridging. Choose **N** (on-demand) if the *DYNASTAR* is to be used as an IP or IPX dial router or bridge.

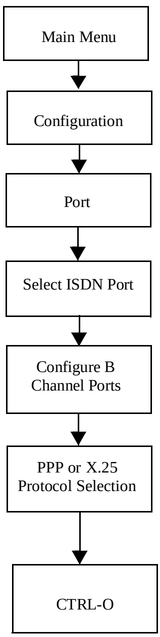
NOTE: Static routes must also be configured to trigger on demand calls. See the section *Routing On Demand Calls* for more information.

11. If **Y** appears in the **Config Required** column, press **<Ctrl-O>** with the cursor on the same line to access the protocol screen that needs to be configured. (Additional configuration is required for an outgoing X.25

line. It is also required for a full time outgoing PPP line.)

✓ The PPP Protocol Configuration screen or the X.25 Protocol Configuration screen (Figure 9-12 or Figure 9-13, respectively) is displayed, depending on your protocol selection.

NOTE: You can apply the X.25 configuration template to an outbound line by first selecting **Use In** or **In/Out** and an inbound telephone number containing the configuration you want. When you save these selections and then return to the Port Configuration menu and choose **Use Out**, the configuration has been applied to the outbound line. The telephone number itself is not applied to the outbound line, however, since the X.121 address included in the configuration will be used to select an outgoing line from the X.121 Address Translation table.You can then adjust the parameters on the outbound X.25 line if you choose and save them with the **Process Selections** command. Changes to the outbound line do not influence the configuration for the Inbound Telephone Number on the ISDN Incoming Telephone Numbers screen, nor do the changes you make on the ISDN Incoming Telephone Numbers screen influence the outbound line you have already configured.




```
                  *** PPP Synchronous Port Configuration ***

Port: 3  ISDN port                              Last changed: 4-23-02  16:23:19

|- Press <RET> to toggle values. -|  |-Type in values. Max chars shown in () --|
Port type:      PPP                  Port name:    ISDN Port 3                 (14)

Connection mode:   FULL TIME    Phone number:                                  (17)
Line speed:        56 Kbps data

Circuit backup:  N




                                                  Process selections (Y/N):  Y

__________[DynaStar_3df2]___________
Use TAB & CURSOR keys to move among fields.   Press ESC to abort command & exit.
```

Figure 9-13   The PPP Protocol Configuration Screen

```
                          ***X.25 Port Configuration***
Port: 3  ISDN Port                               Last changed:  4-23-02  11:26:45

|- Press <RET> to toggle values. -|  |-Type in values. Max chars shown in () --|
Port type:             X.25 line         Port name:    ISDN Port 3              (14)
                                         X.121 Address:                   (15 BCD)
Connection mode:     FULL TIME           Phone Number:
Line speed:          56 kbps data
Number of flags:       (0-15) 0        Allow User Data:              Y
Calling address mod:      NONE         LAPB extended:                N
Local Address insert:        N         X.25 mode:                    DTE
Max Window size:             7         K LAPB window size:           7          (fixed)
Max Packet size:          1024         T1 Acknowledgment timer: 3            (1-255 sec)
Packet/Window Neg:           N         T3 Idle Timer:                30      (0-255 sec)
Require CUG:                 N         N2 Retransmission count:      20         (1-255)
Require NUI:                 N         N1 Max frame size:            8248 bits
Req Reverse Charging:        N         LCN Partition       Base LCN     Number of VCs
Route inbound calls on CUD:  N                             (1-4095)     (2048 total)
Traffic types permitted on line            Permanent:      1            0
     IP Routing:              Y            One-way in:     1            0
     IPX Routing:             N            Two-way:        1            4095
     Ethernet Bridging:       N            One-way out:    4095         0


_______[DynaStar_3614]_______ Save changes and return to previous menu (Y/N): Y
  Use TAB & CURSOR keys to move among fields.    Press ESC to abort command & exit.
```

Figure 9-14   The X.25 Protocol Configuration Screen

12. Configure the protocol screen. For more information on the screen's parameters, see Chapter 6, *The X.25 Application*, or Chapter 10, *The PPP Application*.

NOTE: If you went to the PPP screen, you must also configure an IP address entry in the PPP Dial Directory. See the section on the PPP Dial Directory screen later in this chapter for more information.

13. When you have completed your selections, enter **Y** in the field **Save changes and return to previous menu** and press **<return>**.

✓ You return to the ISDN B Channel Port Configuration screen.

14. Repeat this procedure for any additional B-channels that will be used.

NOTE: Parameter settings need not be the same on the B-channels.

NOTE: You must also configure the X.121 Address table for the X.25 channels you are using and you must set a specific parameter on the Systemwide Parameters screen. These steps are described in the following sections.

Table 9-3 PPP Options on the B-Channel

Parameter	Description	Values
Port type	The type of traffic the port will handle. <return> toggles through permissible values. A menu specific to the type selected appears when the cursor is moved from the field.	PPP, X.25 line Default = PPP
Port name	A name to help you identify this port.	Max 14 chars Default = ISDN Port 3/4

Table 9-3 PPP Options on the B-Channel (cont.)

Parameter	Description	Values
Connection mode	This option is controlled from the B Channel Port Configuration menu. Specifies the type of connection. Full Time should be used for a dedicated connection that will not normally be disconnected. This setting can be used for IP or IPX routing and bridging. On Demand should be selected if the DYNASTAR is to be used as an IP or IPX dial router or bridge. (See also the section *Configuring Routes for On-Demand Calls*.)	Full Time On Demand (Default)
Location name	Appears only for Full Time connection mode. Identifies the remote location to be called. This name must match an entry in the PPP Dial Directory. For more information, see the section *Configuring the Dial PPP Directory* in Chapter 10, *The PPP Application*.	User entry Default = null
Circuit backup	Appears only for Full Time mode. Indicates whether this line is to be backed up by a dial line if it goes down. If enabled, the parameters Backup when line down, Restore when line up, and Backup location name also appear on the screen.	Y N = default
Backup when line down	Appears only if Circuit backup is set to Y. Specifies how quickly this line should be backed up if it goes down.	1-255 seconds 10 = default
Restore when line up	Appears only if Circuit backup is set to Y. Specifies how quickly the backup line should be taken down and this line restored once this line comes back up.	1-255 seconds 30 = default
Backup location name	Appears only if Circuit backup is set to Y. Identifies the line that will be used as the backup line if the PPP line goes down. This line must be configured in the PPP dial directory.	17 characters Default = null

Table 9-3 PPP Options on the B-Channel (cont.)

Parameter	Description	Values
Calls supported	Appears only when the Connection mode is On Demand. Indicates whether Dial-in & out, Dial-in only, or Dial out only connections are allowed.	Dial-in & out Dial-in only Dial out only Default = Dial-in & out
Remote IP address	This is the IP address of the remote client; it appears only when Dial-in & out or Dial-in only is selected. NOTE: These addresses, generally used for Asynchronous PPP connections, are only required if the remote device asks to be assigned an IP address during call setup. If the remote device is a *DYNASTAR*, these options do not need to be filled in.	User entry Default = 0.0.0.0
Remote IPX address	This is the IPX address of the remote client; it appears only when Dial-in & out or Dial-in only is selected. See also the note for the Remote IP address option.	User entry Default = 00000000 Max 8 characters (Hex)
Authenticate remote with PAP/CHAP	Appears only when Dial-in & out or Dial-in only is selected. Indicates whether PAP/CHAP authentication will be used to determine if the remote end is a valid user. See the section *PPP Authentication* in Chapter 10 for more information.	Y N = default
Local PAP/CHAP ID	Appears only when Dial-in & out or Dial-in only is selected. Defines the local PAP/CHAP identification if the local unit is required to provide this information. See the section *PPP Authentication* in Chapter 10 for more information.	max 32 chars Default = null

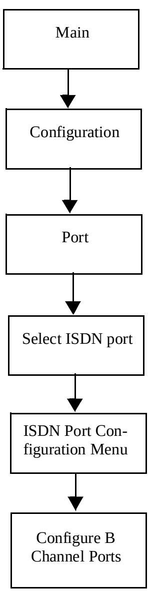
9

ISDN Configuration

B-Channel Assignments and Configuration Order

The order of the B-Channel Port Configuration table is important, since the channels are assigned in order from the top of the table. For example, given the table in Figure 9-15, the first incoming call to a number *other* than 703 280-1946 will be assigned to channel port 106 if it is free. If 106 is not free, the call will be assigned to port 107 (if 107 is free) and so on.

A second rule has impact on this order, however. For incoming calls, the *DynaStar* tries to assign the call to a port with Use=In and then, if no such port is available, to a port with Use=In/Out. For outgoing calls, the unit first attempts to assign the call to a port with Use=Out and then, if no such port is available, to a port with Use=In/Out.



ISDN B Channel Port Configuration

ISDN Interface: Slot 0 T1/PRI 1 Last changed: 1/6/97 1335:44

Port	Use	Inbound Tel #	Protocol	Class	ML	Full Time	Config Required
101	OUT		PPP		N	N	
102	OUT		PPP		Y	Y	
103	IN	7032801946	X.25				
104	IN/OUT	7032801946	X.25		Y		
105	OUT		X.25		Y	NY	
106	IN	DEFAULT	PPP		N		
107	IN/OUT	DEFAULT	PPP		Y		
108	IN/OUT	DEFAULT	PPP		Y		
109	IN/OUT	DEFAULT	PPP		Y		
110	IN/OUT	DEFAULT	PPP		Y		
111	IN/OUT	DEFAULT	PPP		Y		
112	IN/OUT	DEFAULT	PPP		Y		
113	IN/OUT	DEFAULT	PPP		Y		
114	IN/OUT	DEFAULT	PPP		Y		
115	IN/OUT	DEFAULT	PPP		Y		

_______[DynaStar dc000345]_______ Process B channel port configuration (Y/N): Y

To DELETE an entry use <CTRL-D>. To configure port options use <CTRL> O.

Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.

Figure 9-15 Example B-Channel Port Configuration Screen

MULTILINK PPP

Multilink PPP enables interleaving of packets over two ISDN B-channels to provide an effective wire speed of 112 or 128 kbps. Multilink PPP is configured on the PPP Dial Directory menu. For additional information, see the section *Configuring the PPP Dial Directory* in Chapter 10, *The PPP Application*.

■ CHANNELIZED T1/E1/PRI CONFIGURATION

The procedure that follows explains how to configure your T1/E1/PRI card to support channelized T1/E1. Configuration consists of defining physical level parameters for the T1/E1 trunk, mapping time slots to channels, and then defining the parameters for the designated channels. Each time slot can be assigned to one channel, and each channel can have from 1 to 24 time slots for T1, or from 1 to 31 time slots for E1. The time slots can be assigned to the channels in any combination of n x 64 or n x 56 kbps (T1 only) to support X.25, PPP, or frame relay traffic.

Before you begin the configuration procedure, you should know how you intend to define the available time slots. For example, you might assign time slots 01 through 04 to channel 101 and configure this “port” for the X.25 protocol; time slots 05 and 06 to channel 102 to be used with the PPP protocol; and time slots 07 through 11 to channel 103 and frame relay.

NOTE: It is not necessary to assign consecutive time slots to a channel.

The following procedure discusses the configuration of a channelized T1 trunk. The configuration of an E1 trunk is very similar. Differences in the procedure and screens are explained in the subsection *E1 Configuration*.

Assigning Network Parameters and Time Slots for a Trunk

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) appears.

2. From the Configuration Commands menu, select **Port**.

✓ A list of available ports appears.

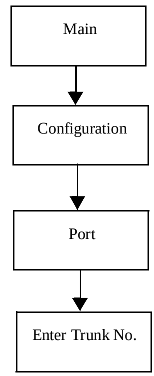
3. Enter **x00 <return>** (100 in the example given in Figure 9-16) to configure the first T1 trunk or **x50** (e.g., 150) to configure the second trunk.

✓ If you are configuring a channelized T1 trunk, the T1 Trunk Parameters Screen, shown in Figure 9-16, is displayed.

✓ If you have previously configured a full Primary Rate Interface trunk, the ISDN Port Configuration Menu, shown in Figure 9-17, is displayed.

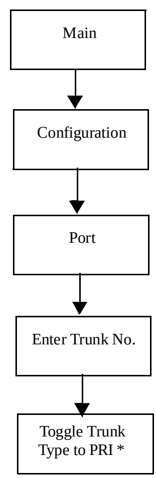
```
                    ***T1 Trunk Parameters***
                        [Channelized only]

Port: 100                                  Last Changed  : 4-23-02   23:45:00
Trunk Type:    T1 channelized              Trunk Name     : Trunk 1/1           (14)

Frame Type:    ESF                         Time Slot Bandwidth:    64 kbps
Line Coding:   B8ZS                        Yellow Alarm Mode:      FDL
CRC 6:         On                          Line Build Out:         0 to 133 ft
                                           Transmit clk source:    Local oscill.



------------------------------------------Time Slot Assignments------------------------------------------
01: 101     05: 102     09: 103     13: ----     17: ----     21: ----
02: 101     06: 102     10: 103     14: ----     18: ----     22: ----
03: 101     07: 103     11: 103     15: ----     19: ----     23: ----
04: 101     08: 103     12: ----    16: ----     20: ----     24: ----


_______[DynaStar dc000345]_______                  Process selections (Y/N): Y
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 9-16   T1 Trunk Parameters Screen




```
                    ***T1 Trunk Parameters***
                          [PRI Capable]
Port: 100                                  Last changed  : 4-23-02   23:45:00
Trunk Type:    T1 PRI                      Trunk Name    :   Trunk 1/1          (14)

Frame Type:         ESF                    D Channel Bandwidth:   64 Kbps
Line Coding:        B8ZS                   Yellow Alarm Mode:     FDL
CRC 6:              On                     Line Build Out:        0 to 133 ft
                                           Transmit Clk source:   Local oscill.
Signaling Type:     NI-1
Device Type:        USER



_______[DynaStar dc000345]_______                  Process selections (Y/N): Y
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 9-17   T1 Trunk Parameters for PRI Board



* Or select Configure D Channel from ISDN Port Configuration menu.

✓ The type of T1 daughterboard installed is indicated just below the menu name as Channelized only or PRI capable.

4. If the T1 or E1 Trunk Parameters menu (Figure 9-16) is displayed, go to Step 9.

5. If you see the ISDN Port Configuration screen and want to configure a channelized interface, select **Configure PRI/BRI D Channel Port and layer 1 parameters**.

✓ The **T1** or **E1 Trunk Parameters** screen is displayed.

6. Select **T1** or **E1 channelized** as the **Trunk Type**.

✓ The screen changes to reflect your selection. (It should now look similar to Figure 9-16.)

7. Move the cursor to **Process Selections**, select **Y**, and press **<return>**.

✓ A message screen appears saying that the channels will be reinitialized. Press **<return>** and you return to the Configure Port menu.

8. Enter your port number.

✓ The T1 Trunk Parameters screen (Figure 9-16) appears.

9. In the top portion of the T1 Trunk Parameters screen, define the parameters as required by your network. Values should be set up to agree with the other end of the connection. Table 9-2 gives a list of all parameters and possible values.

10. In the Time Slot Assignments section of the screen, toggle to enter the channel that will be assigned to each time slot, or type in the channel number.

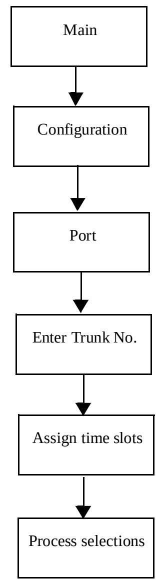
    NOTE: To clear a timeslot assignment, move the cursor to the field and enter a 0, a -, or a space, followed by **<return>**.

11. When you have completed your configuration, type **Y** at the **Process selections** prompt to save and quit.

✓ If you have made changes in time slot assignments, a Port Configuration screen that lists all possible channels, similar to the one in Figure 9-18, appears. The ports that have been changed are noted at the bottom of the menu.

```
                         ***Configure Port***

Valid port numbers (with names) are:
100: Trunk 1/1        116: TDM chan 116   150: Trunk 1/2        166: TDM chan 166
101: TDM chan 101     117: TDM chan 117   151: TDM chan 151     167: TDM chan 167
102: TDM chan 102     118: TDM chan 118   152: TDM chan 152     168: TDM chan 168
103: TDM chan 103     119: TDM chan 119   153: TDM chan 153     169: TDM chan 169
104: TDM chan 104     120: TDM chan 120   154: TDM chan 154     170: TDM chan 170
105: TDM chan 105     121: TDM chan 121   155: TDM chan 155     171: TDM chan 171
106: TDM chan 106     122: TDM chan 122   156: TDM chan 156     172: TDM chan 172
107: TDM chan 107     123: TDM chan 123   157: TDM chan 157     173: TDM chan 173
108: TDM chan 108     124: TDM chan 124   158: TDM chan 158     174: TDM chan 174
109: TDM chan 109                         159: TDM chan 159
110: TDM chan 110                         160: TDM chan 160
111: TDM chan 111                         161: TDM chan 161
112: TDM chan 112                         162: TDM chan 162
113: TDM chan 113                         163: TDM chan 163
114: TDM chan 114                         164: TDM chan 164
115: TDM chan 115                         165: TDM chan 165
                      Changes made for port 100
                      Enter another port number:
_______[DynaStar dc000345]_______
Terminate input with <RET>.               Press ESC to return to previous menu.
```

Figure 9-18   Port Configuration Screen Listing all Channels



SETTING PARAMETERS FOR INDIVIDUAL CHANNELS

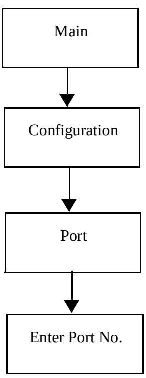
Now configure the parameters for each T1 channel to which you assigned time slots in the previous procedure.

NOTE: If you are starting from a screen other than the Configure Port menu that lists all of the channels on the trunk (see example in Figure 9-18), see the section *Modifying T1 or E1 Port Parameters* later in this chapter.

1. At the **Enter another port number** prompt on the Configure Port screen, enter the number of the first channel that you want to configure (for example, 101).

✓ The X.25 Port Configuration screen shown in Figure 9-19 appears.

NOTE: X.25 is the default protocol for these ports. A different configuration screen might appear if the port has been previously configured to a different protocol.




```
                          ***X.25 Port Configuration***
 Port: 101 TDM channel                          Last changed:  4-23-02 11:26:45

|- Press <RET> to toggle values. -|  |-Type in values. Max chars shown in () --|
Port type:           X.25 line             Port name:   TDM chan 101           (14)
                                           X.121 Address:    24101          (15 BCD)

Line speed:    256 kbps (4x64K)        Non-Zero DTE Cause:        N
Number of Flags:(0-15)          0      Allow User Data:           Y
Calling address mod:         NONE      LAPB extended:             N
Local address insert:           N      X.25 mode:                 DTE
Max Window size:                7      K LAPB window size:        7          (fixed)
Max Packet size:             1024      T1 Acknowledgment timer:   3      (1-255 sec)
Packet/Window Neg:              N      T3 Idle timer:             30     (0-255 sec)
Require CUG:                    N      N2 Retransmission count:   20         (1-255)
Require NUI:                    N      N1 Max frame size:         8248 bits
Req Reverse Charging:           N       LCN Partition     Base LCN      Number of VCs
Route inbound calls on CUD:  N                           (1-4095)
Traffic types permitted on line            Permanent:      1                  0
     IP Routing:           Y                One-way in:     1                  0
     IPX Routing:          Y                Two-way:        1                  4095
     Ethernet Bridging:    Y                One-way out:    4095               0


 _______[DynaStar_3614]_______                   Process selections (Y/N): Y
  Use TAB & CURSOR keys to move among fields.   Press ESC to abort command & exit.
```

Figure 9-19 Sample Configuration Screen for T1 Channel

2. Toggle the Port Type field until the protocol you want to define (PPP, X.25, or frame relay) is displayed and press **<tab>** or an arrow key.

✓ The port configuration screen for the selected protocol appears.

NOTE: The fields in these screens are the same as those in the configuration screens for any port of this type, with the following exceptions: There is no Connection Mode field (DTE, DCE, Dial); and the line speed is calculated based on what you configured on the T1 Trunk Parameters screen.
For example, in Figure 9-19, the line speed shown is 256 because four 64 K timeslots

were assigned to Port 101 on the T1 Trunk Parameters screen (Figure 9-16). If the T1 trunk time slot bandwidth is set to **Either**, you can toggle between Nx56K and Nx64K rates. Otherwise, the line speed cannot be changed.

3. Complete the parameters as required for your network. For information on parameters and values, see Chapter 6, *The X.25 Application* or Chapter 10, *The PPP Application*.

4. When you have completed the channel configuration, enter **Y** at the **Process Selections** prompt to save and exit.

✓ You return to the Port Configuration screen (Figure 9-18).

5. Repeat this procedure for each of the channels that you assigned in the T1 Trunk Parameters Screen.

NOTE: Each channel defined in the T1 Trunk Parameters Screen must have its parameters individually configured on the appropriate port configuration screen.

E1 CONFIGURATION

The E1 Configuration is identical to T1 channelized configuration, described in the previous sections, except that there are 31 possible time slots to assign, as shown in the E1 Trunk Parameters screen in Figure 9-20. In addition, some fields found on the T1 screen are not on the E1 screen, and some values for the parameters are different. These are detailed in Table 9-2.

CAUTION: When CAS (Channel Associated Signaling) frame mode is selected on the trunk configuration screen, time slot 16 is used for signaling and is not available for a channel assignment. (In this case, only 30 time slots are available.)

Modifying T1 or E1 Port Parameters

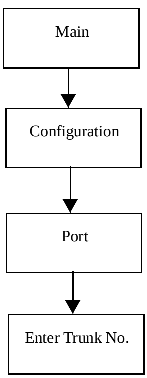
To modify parameters on a previously configured port:

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu is displayed.

2. Select **Port**.

✓ The Configure Port menu (similar to Figure 9-5) is displayed.




```
                         ***E1 Trunk Parameters***
                              [PRI Capable]

Port: 400                                      Last changed: 4-23-02 23:45:00
Trunk Type:    E1 channelized                  Trunk Name: Trunk 4/1          (14)

Frame Type:    FAS
Line Coding:   HDB3
CRC4:          On                              Interface type:    120 Ohm Balanced
                                               Transmit Clk source:     Local oscill.



-----------------------------------------Time Slot Assignments-----------------------------------------
01: ----      06: ----      11: ----      17: ----      22: ----      27: ----
02: ----      07: ----      12: ----      18: ----      23: ----      28: ----
03: ----      08: ----      13: ----      19: ----      24: ----      29: ----
04: ----      09: ----      14: ----      20: ----      25: ----      30: ----
05: ----      10: ----      15: ----      21: ----      26: ----      31: ----
                            16: ----

_______[DynaStar dc000345]_______                 Processselections(Y/N): Y
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 9-20 E1 Trunk Parameters Screen

3. Enter the Port number.

✓ The Port Configuration screen for that port is displayed.

4. Modify parameters as required.

NOTE: The fields in these screens are the same as those in the configuration screens for any port of this type, with the following exceptions: There is no Connection Mode field (DTE, DCE, Dial); and the line speed is

calculated based on what you configured on the T1 Trunk Parameters screen.
For example, in Figure 9-19, the line speed shown is 256 because four 64 K timeslots were assigned to Port 101 on the T1 Trunk Parameters screen (Figure 9-16). If the T1 trunk time slot bandwidth is set to **Either**, you can toggle between Nx56K and Nx64K rates. Otherwise, the line speed cannot be changed.

5. Enter **Y** in the **Process selections** field and press **<return>** to save your changes.

✓ You are returned to the T1 or E1 Port Configuration screen (see example in Figure 9-18).

PPP Dial Directory Screen and IP Information Screen

The PPP Dial Directory screen needs to be configured for outgoing PPP calls when **Full Time** is set to **Y** on the B Channel Port Configuration screen. Among other things, the PPP Dial Directory screen identifies the IP address for the source and the destination (Local IP address and Remote IP address, respectively). Whenever possible (for example, when setting up a new network with all DynaStar equipment), all the source and destination IP addresses should be on the same network (Figure 9-21).

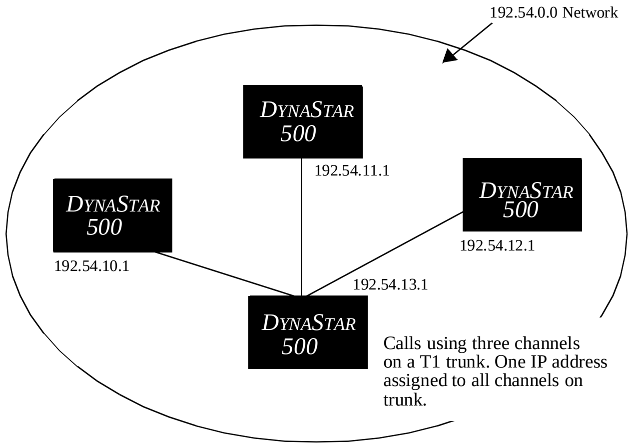


Figure 9-21 Network Showing All Equipment on Same IP Network

When all the equipment is on the same network, you can set the IP address for the T1/E1 trunk in the IP Port Information screen (Figure 9-22) and use this address for all channels on the trunk. Using the example from Figure 9-21, you would enter the IP address 192.54.13.1 for Trunk 1/1 (if you were using the first trunk), or for Trunk 1/2 (if you were using the second trunk) in the IP Port Information screen. This address will then appear in the PPP Dial Directory Entry screen (Figure 9-23) in the Local IP address field when the **ISDN Interface** field is set to the appropriate trunk.

```
                         ***IP Port Information**
                                         Last changed: 4-23-02 12:15:21

 Port(s)     Interface      IP Address      IP Mask       |-Use RET to toggle
                            x.x.x.x         x.x.x.x       Protocol   Encaps
       0     Ethernet       0.0.0.0         0.0.0.0         RIP      Enet II
   2 - 4     D Channel      0.0.0.0         0.0.0.0         RIP
       5     HS WAN         0.0.0.0         0.0.0.0         RIP
 101-124     Trunk 1/1      192.54.13.1     0.0.0.0         RIP
 151-174     Trunk 1/2      0.0.0.0         0.0.0.0         RIP







 ________[DynaStar_3614]_________              Process IP addresses (Y/N): Y
Lines with port ranges are multiport interfaces. Configure these ports together
on one line. Or with cursor on line, press <CTRL-O> to configure separately.
*Fields are blank on this screen if ports are configured separately.
```

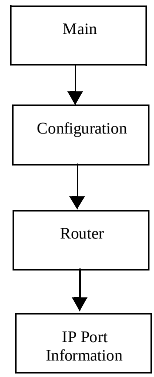


Figure 9-22 IP Port Information Screen Showing T1 Trunk

```
                       ***PPP Dial Directory Entry***

 | --Press <RET> to toggle values. --|  | –Type in values. Max chars shown in ( ) --|

                                      Location name:                          (17)
 Dialing type:     ISDN               ISDN Interface:  100 - Trunk 1/1
 Call data rate:  56 kbps data        Phone Number:                           (21)

 Authenticate remote with PAP:   N    CHAP:   N
 Local PAP/CHAP ID:                                                    (32 ASCII)

 Traffic type permitted on call
      IP Routing:            Y           Remote IP address:    0.0.0.0
      Ethernet Bridging:     N           Local IP address:     192.54.13.1
                                         Local mask address:   0.0.0.0
      IPX Routing:           N
 Compression:                N

 IP Routing Protocol:          NONE
 Use as default IP route:      N

________[DynaStar_3614]_________                  Process selections (Y/N): Y
Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

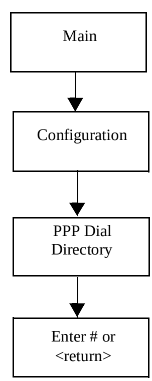


Figure 9-23 PPP Dial Directory Configuration Screen

If a channel needs an individual IP address assignment (this will be the case if your destinations are on multiple networks, as shown in Figure 9-24, or if a channel is configured as X.25 outgoing), you can individually define the IP addresses by entering <CTRL-O> on the line of the appropriate trunk in the IP Port Information screen. This will take you to the additional screen shown in Figure 9-25.

You can access multiple networks because the IP addresses are assigned to telephone numbers rather than to physical ports. On a BRI, this also lets you communicate with more than two different locations, each with differentWAN network addresses. There can only be two simultaneous connections (because the BRI supports only two B-channels), but at different times it is possible to connect to *n* different sites if you configure the PPP Dial Directory screen to do this.

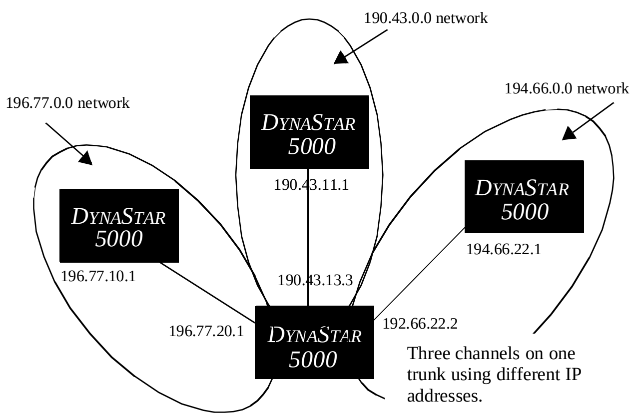
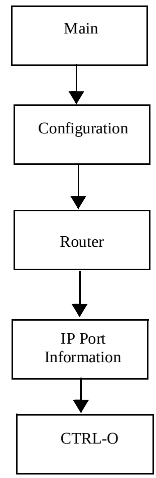


Figure 9-24 Network Showing IP Destinations on Multiple Networks

```
***IP Interface (100) Trunk 1/1***
                                          Last changed: 1/9/97 12:15:21

Port(s)     Interface       IP Address      IP Mask      |-Use RET to toggle
                            x.x.x.x         x.x.x.x      Protocol    Encaps
   101    TDM chan 101    0.0.0.0         0.0.0.0         RIP
   102    TDM chan 102    0.0.0.0         0.0.0.0         RIP
   103    TDM chan 103    0.0.0.0         0.0.0.0         RIP
   104    TDM chan 104    0.0.0.0         0.0.0.0         RIP
   105    TDM chan 105    0.0.0.0         0.0.0.0         RIP
   106    TDM chan 106    0.0.0.0         0.0.0.0         RIP
   107    TDM chan 107    0.0.0.0         0.0.0.0         RIP
   108    TDM chan 108    0.0.0.0         0.0.0.0         RIP
   109    TDM chan 109    0.0.0.0         0.0.0.0         RIP
   110    TDM chan 110    0.0.0.0         0.0.0.0         RIP
   111    TDM chan 105    0.0.0.0         0.0.0.0         RIP
   112    TDM chan 105    0.0.0.0         0.0.0.0         RIP
   113    TDM chan 105    0.0.0.0         0.0.0.0         RIP
   114    TDM chan 105    0.0.0.0         0.0.0.0         RIP
   115    TDM chan 105    0.0.0.0         0.0.0.0         RIP

________[DynaStar_3614]_________          Keep new IP addresses (Y/N): Y
You can configure each port of a multiport interface separately on this
screen.
Press ESC to return to the previous screen.
```

Figure 9-25 IP Port Information Screen for Individual Port Assignments



The PPP Dial Directory screen, shown in Figure 9-23, contains several fields to accommodate ISDN configurations. The **Dialing Type** field can be set to **ISDN**. When this is the case, the **ISDN Interface** field must be configured. This field indicates which ISDN line should be used for the outgoing call, and it can be set to the BRI interface, or any PRI interface available in your unit.

Since the B-channels are no longer configured individually in conjunction with a physical port, you can configure the local IP address with the dial directory entries (if you have configured a global address in the IP Port Information screen, it will show up here when the corresponding interface is selected in the **ISDN Interface** field). There are also entries for the local mask address and the remote IP address.

DIRECTORY NUMBER MATCHING. The *DYNASTAR* compares the directory number you enter on the ISDN Incoming Telephone Numbers menu to the Dialed Number Information in an incoming call setup message. As a result,

calls are directed to the correct port, and the *DynaStar* is prevented from answering calls directed toward another device.

When a called number is compared to the directory number, it does not have to be an exact match. Instead, the shorter of the two numbers is used as the key and the numbers are matched from right to left. If the **Directory number** field contains the word DEFAULT, all calls will be accepted and assigned to either Port 3 or Port 4.

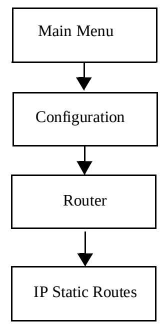
Table 9-4 provides some matching examples:

Table 9-4 Directory Number Matching Examples

Directory Number	Dialed Number Information Entry	Result
555-1212	(703) 555-1212	Match
(703) 555-1212	555-1212	Match
(703) 555-1212	(703) 555-1211	No Match

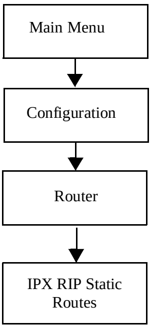
Configuring Routes for On-Demand Calls

If you are configuring the B-channel for on demand (dial router) use, you must also create entries in the IP Static Routing table (Figure 9-26) or the IPX RIP Static Routing table (Figure 9-27). For an IPX entry, you must configure a Next Network address; for an IP entry, you must configure a Next Hop address.



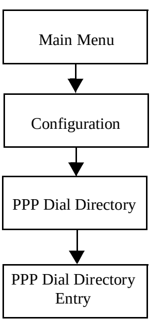

```
                                    ***IP Static Routes***
                                                    Last changed:  2/1/99  11:26:45
         IP Address              IP Mask          Next Hop                Hops
         x.x.x.x                 x.x.x.x          x.x.x.x                 (0-15)
1:
2:
3:
4:
5:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:
Note: x = 0-255

 ________[DynaStar_3614]_________                  Process Static Routes (Y/N): Y
 In IP address field, use UP/DOWN to scroll and LEFT to process selections.
 To change or add entry, enter new value.          Use <CTRL-D> to delete entry.
 Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 9-26 IP Static Routes Table




```
                         ***IPX RIP Static Routes***
                                            Last changed:  4-23-02  11:26:45

     Remote Destination      Next Network        # of Hops to       Delay
     Network Number          in the Route        Next Network       Ticks
     (8 HEX Digits)          (8 HEX Digits)      (1-15)             (1-360)
1:   00000001                00000002               1                  60
2:
3:
4:
5:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:

 ________[DynaStar_3614]_________          Process RIP static routes (Y/N): Y
In server name field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.          Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 9-27   IPX RIP Static Routes Menu

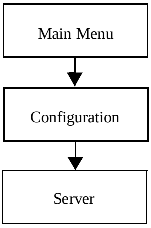



```
                         ***PPP Dial Directory Entry***

 | --Press <RET> to toggle values. --|  | –Type in values. Max chars shown in ( ) --|
                                         Location name:test                        (17)
 Dialing type:      ISDN                 ISDN Interface:       500- Trunk 5/1
 Call data rate:  56 kbps data           Phone Number:                             (21)

 Authenticate remote with PAP:   N       CHAP:   N
 Local PAP/CHAP ID:              N                                          (32 ASCII)

 Traffic type permitted on call
       IP Routing:            Y             Remote IP address:   0.0.0.0
       Ethernet Bridging      N              Local IP address:    0.0.0.0
                                             Local Mask address:  0.0.0.0
       IPX Routing:           Y
 Compression:N


 IP Routing Protocol:          NONE
 Use as default IP route:      N

________[DynaStar_3614]_________                   Process selections (Y/N): Y
Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 9-28   PPP Dial Directory Entry

In addition, you must create a PPP Dial Directory entry (Figure 9-28) for the IP Next Hop (entered as the **Remote IP Address** on the Dial Directory screen) or the IPX Next Network address (entered as the **Novell Network Number** on the Dial Directory screen) and define the destination **Phone Number** that will be called for that hop. Then, when a call is received on the B-channel, the address is checked against static routes. Once the Next Hop or Next Network is found in the Static Routes Table, it is located in the Dial Directory entries, and a call is established to the phone number you have specified. For more information on IP and IPX Static Routes, see Chapter 12, *The IP/IPX Router Application*.

INACTIVITY TIMER. When you place an On Demand call on a B-Channel, the ISDN call clears automatically after a period of inactivity. This period is defined in the **B Channel call time-out** field on the Systemwide Parameters menu (Figure 9-29), which is accessed from the Server menu. When this timer expires, the entire BRI interface (both B-channels and the D-channel) is disabled. To reenable the BRI, you must reenable Port 2. For more information on system parameters, see Chapter 4, *System Functions and Parameters*.




```
                    *** Systemwide Parameters***

Server name: DynaStar399c                                                   (47)
Supervisor console herald:        DynaStar Supervisor                       (32)
Dial IP idle timer:               2             (0-disable, 1-254 min, 255-10 sec)
Dial IPX idle timer:              2                         (0-disable, 1-255 min)
Dial Bridge idle timer:           2                         (0-disable, 1-255 min)
B Channel call timeout:           0                        (0-disable, 1-1440 min)
X.25 call set-up timer:           5                                    (1-30 min)
XOT Idle Timer                    0                          (0-disable, 1-30 min)
PPP IP prioritization:            0                             (0 - disable, 1-99)
IPX-In preferred File Server:                                               (47)
IPX-Out broadcast address:        399c                                       (8)
Reserved LCNs:                    N                                <CR> to toggle
Exhaustive Routing:               ENDPOINT                         <CR> to toggle
X32 No LCN Drop Timer:            6                         <0-disable, 1-12<10 sec>>
Daughter Board Auto-Recover:      Y                                <CR> to toggle


_______[DynaStar 399c]_______                       Process selections (Y/N): Y
Use <TAB> and CURSOR to move fields.   Press ESC to return to previous menu
```

Figure 9-29   Systemwide Parameters Screen

Configuring the X.121 Routing Table

When configuring X.25 over ISDN, you must also configure the X.121 Routing table:

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu is displayed.

2. Select **X.25**.

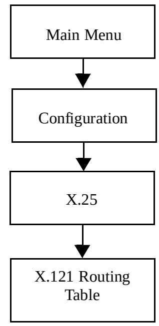
✓ The X.25 Commands menu is displayed.

3. Select **X.121 routing table**.

✓ The X.25 Concentrator Routing table (Figure 9-30) is displayed.

```
                        ***X.25 Concentrator Routing Table***
                                              Last changed: 4-23-02  7:00:45

  X.121 address    Shared   |------Use RET to Toggle------|    X.32 dial line phone #
 (1-15 BCD D&X)  Scheme    Port      Priority    Dial Speed        (max 19 characters)
1:
2:
3:
4:
5:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:
_______[DynaStar 35dd]_______                        Process Routing Tables (Y/N):
Search for X.121 address:                                 SelectShareScheme:
To change or add entry, enter new value.                 Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 9-30   X.25 Concentrator Routing Table



4. Enter the X.121 address for Port 3 and, if it will be used, Port 4.

5. Specify the dial speed.

6. If this is an **On Demand** connection (as specified in the **Connection mode** field on the Port Configuration menu for the B-channel), enter the related destination phone number in the field **X.32 dial line phone number**.

NOTE: If you do not enter the **X.32 dial line phone number** for an On Demand connection, the routing table entry will not be saved.

NOTE: Be sure the PAD port is configured correctly. If you are configuring Port 6 on a remote *DYNASTAR 100i* as the X.25 destination, the port must be configured as a PAD port and must be given an X.121 address on the X.25 Concentrator Routing table.

9

ISDN Configuration

Busy/Unbusy Trunks

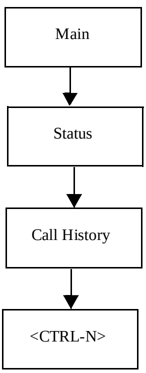
To busy out a trunk, or to return a busy trunk to service:

1. From the Main menu, select **Status**.

✓ The Status commands menu (Figure 3-7) appears.

2. From the Status commands menu, select **Call History**.

✓ The ISDN PRI Call History screen (Figure 9-31) appears.f




```
                          ***ISDN PRI Call History***
                                              Last Reset: 5-29-02 19:29:50
Current Slot 1 & 2
Active Channels
Port     State channel        1 1 1 1 1 1 1 1 1 1  2 2 2 2 2 2 2 2 2 2 3 3
                      1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Trunk 1/1 OK  _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Trunk 1/2 OK  _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Trunk 2/1 OK  _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Trunk 2/2 OK  _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

History          Trunk 1/1    Trunk 1/2    Trunk 2/1    Trunk 2/2    Total
# ISDN call    :     0            0           10           10          20
# Total succ.  :     0            0           10           10           0
# Port unav    :     0            0            0            0           0
# Modem unav   :     0            0            0            0           0
# ISDN fail    :     0            0            0            0           0
# Handskfail   :     0            0            0            0           0
# Neg fail     :     0            0            0            0           0

  Press <CTRL-B> to Busy/Unbusy Trunk
  Press <CTRL-A> to clear all statistics        Press <CTRL-N> for next screen.
  _______[DynaStar dc000345]_______            Press<RET>forstatisticsupdate.
   Press <ESC> to return to previous menu.      Press <CTRL-D> to clear statistics.
```

Figure 9-31 ISDN PRI Call History Screen

3. From the ISDN PRI Call History screen, enter **<CTRL-B>**.

✓ You are prompted for a trunk number.

4. Enter a specific trunk number. Or enter **0** to busy out all trunks. Press **<return>**.

✓ The new state of the trunk is displayed on the ISDN PRI Call History menu.

- ✓ If the specified trunk or trunks were previously available, they are marked busy and cannot accept new calls.

  If the trunk or trunks specified were busy, they are returned to service and will accept new calls.

THE PPP APPLICATION

■ OVERVIEW

PPP (Point-to-Point Protocol) is a data link layer protocol for a point-to-point link. PPP has a multiplexing capability that allows multiple protocols, such as IP and IPX, to share the same link simultaneously. PPP can be used on both synchronous and asynchronous lines.

- Asynchronous PPP gives PC or workstation users remote access to an IP Ethernet network over either dial-up or direct serial communications lines, as shown in Figure 10-1. Asynchronous PPP is widely preferred to SLIP because it provides good error detection and recovery mechanisms, as well as improved security. Both dial-in and dial-out asynchronous PPP are supported.

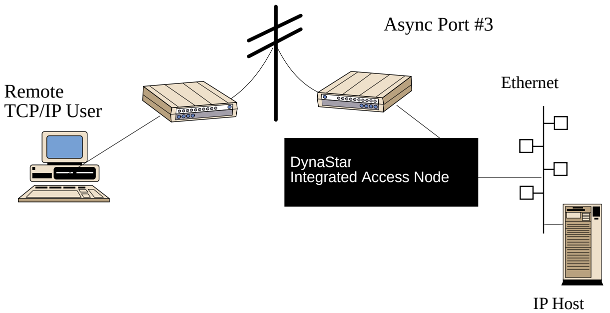


Figure 10-1 Sample Asynchronous PPP Network Configuration

- Synchronous PPP can provide connections for a remote TCP/IP user over a WAN port, as shown in Figure 10-2. Both dedicated and dial synchronous PPP are supported.

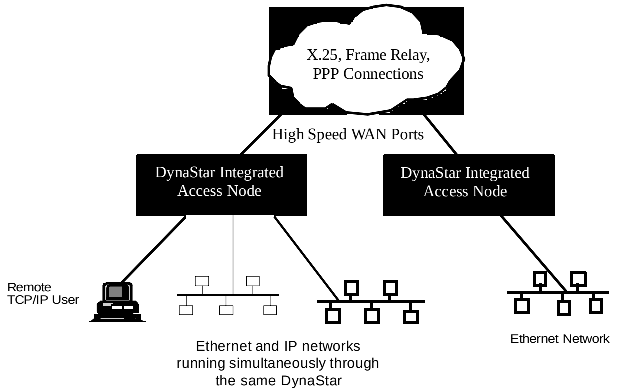


Figure 10-2 Synchronous PPP over WAN Ports

- Multilink PPP (RFC 1717) is based on a Link Control Protocol (LCP) option negotiation that allows a system to indicate to its peer that it is capable of combining multiple physical links into a “bundle.” Multilink PPP enables the interleaving of packets over two ISDN B-channels to provide an effective wire speed of 112 kbps or 128 kbps.

■ Port Configuration

To use PPP as the underlying protocol for bridge or router traffic, you must first configure at least one of the ports in your *DynaStar* to support PPP. The procedures below step you through the configuration process. A complete description of the PPP port configuration parameters for dedicated lines is given in Table 10-1 and for dial lines in Table 10-2. See Chapter 9, *ISDN Configuration*, for the port configuration of an ISDN PPP line.

DEDICATED PPP LINE CONFIGURATION

This section explains how to set up a dedicated PPP line. The line can be synchronous or asynchronous, but synchronous lines are more commonly used as dedicated lines and asynchronous lines are more commonly used as dial lines. Dial line configuration is explained in the next section.

1. From the Main menu, select **Configuration.**

✓ The Configuration Commands menu (Figure 3-11) appears.

2. Select **Port**.

✓ A list of available ports appears.

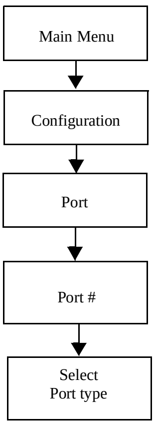
3. Select the port that you want to configure with the PPP protocol and enter that port's number in the **Enter port number** field.

NOTE: You must select a port that is capable of handling the dedicated PPP protocol. This is normally a synchronous port, but could be an asynchronous port. Synchronous PPP can run on any WAN port. If you intend to configure multilink PPP, you must use an ISDN port. (See Chapter 9, *ISDN Configuration*, for more information.)

✓ A menu showing the port parameters that are currently set for the port appears.

4. If the port is not currently configured as PPP, toggle the **Port type** field until **PPP** or **Async PPP** appears and press **<tab>**.

✓ The screen displays the parameters that need to be configured for the PPP line, as shown in Figure 10-3.




```
                    ***PPP Synchronous Port Configuration***
Port:  5  IS-35                                   Last changed:  4-23-02  11:26:45

|---  Press <RET> to toggle values  --||--- Type in values.  Max chars shown in ()  ---|
Port type:       PPP                Port name:      HS WAN                          (14)

Connection mode:        DTE

Line speed:             56.0 kbps
Compression             N
Circuit backup:         N

Traffic types permitted on line
    IP Routing:             Y
    IPX Routing:            Y
    Ethernet Bridging:      Y

Authenticate remote with PAP: N         CHAP: N
Local PAP/CHAP ID:                                                           (32 ASCII)



________[DynaStar_3614]_________                  Process selections (Y/N): Y
 Use TAB & CURSOR keys to move among fields.   Press ESC to abort command & exit.
```

Figure 10-3 PPP Port Parameters Screen for Dedicated Lines

5. In the **Port name** field, enter a name that will help you identify this port. This name will subsequently appear in any list of the ports, such as the list from which you select a port to configure.

6. Enter the connection mode for this line. **DTE** means that the port is a physical DTE device looking for an external clock source. **DCE** means that the port is a physical DCE that provides clocking. (See the next section for configuring dial lines.)

   NOTE: If you are testing asynchronous PPP in direct connection mode, use a straight-through cable. If you are testing in leased mode, use a null modem cable.

7. Indicate whether or not compression is to be used.

NOTE: Compression is most effective on lines operating at lower speeds and used to transfer text files. When compression is used, the devices at each end of the PPP link must support the LZS compression protocol. *DynaStar* products with software version 4.01 and later support this protocol.

8. If the PPP line is to be backed up by a dial line if the PPP line goes down, select **Y** for **Circuit backup**.

9. If you enabled **Circuit backup**, additional fields appear on the screen. Configure these to indicate when to back up and restore the line and to identify the backup line.

10. Select the traffic types to be permitted on the line in the **Traffic types…** field.

11. If you are using PAP or CHAP, configure the parameters as required. (See the section *PPP Authentication* later in this chapter for detailed information.)

12. When your configuration is complete, enter **Y** in the **Process selections** field and press **<return>**.

✓ For dedicated lines (**Connection mode** is set to **DTE** or **DCE**), your configuration is complete.

Table 10-1 Dedicated Line PPP ParameterValue s

Parameter	Description	Values
Port type	The type of traffic the port will handle. **<return>** toggles through permissible values. A menu specific to the type selected appears when the cursor is moved from the field.	Depends on line type
Port name	A name to help you identify this port.	Max 14 chars
Connection mode	The physical level connection of the port. DCE means that the port is a physical DCE that provides clocking. DTE means that the port is a physical DTE device looking for an external clock source. See the next section for information on Dial lines.	DTE=default DCE Dial

Table 10-1 Dedicated Line PPP Parameter Values (cont.)

Parameter	Description	Values
Line speed	The speed of the line.	9600 bps - 2.048 Mbps 56k=default
Compres-sion	Indicates whether compression will be used for the IP traffic on this line. To use compression, you must enable LZS Link Compression in the Applications menu under System Functions (see Chapter 4, *System Functions and Parameters*).	Y N=default
Circuit backup	Indicates if this line is to be backed up by a dial line if it goes down. If enabled, the parameters Backup when line down, Restore when line up, and Backup location name also appear on the screen.	Y N=default
Backup when line down	Specifies how quickly this line should be backed up if it goes down. Appears only if Circuit backup is set to Y.	1-255 seconds 10=default
Restore when line up	Specifies how quickly the backup line should be taken down and this line restored once this line comes back up. Appears only if Circuit Backup is set to Y.	1-255 seconds 30=default
Backup location name	Identifies the line that will be used as the backup line if the PPP line goes down. This line must be configured in the PPP dial directory.	17 characters Default=null
Traffic types permitted on line	Indicates whether IP, IPX, and/or Ethernet bridged traffic are allowed on this PPP line.	Y=default N
Authenti-cate remote with PAP/CHAP	Indicates whether PAP/CHAP authentication will be used to deter-mine if the remote end is a valid user. See the section *PPP Authentication* later in this chapter for more information.	Y N=default

Table 10-1 Dedicated Line PPP Parameter Values (cont.)

Parameter	Description	Values
Local PAP/CHAP ID	Defines the local PAP/CHAP identification if the local unit is required to provide this information. See the section *PPP Authentication* later in this chapter for more information.	max 32 chars Default=null

Dial PPP Line Configuration

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. Select **Port**.

✓ A list of available ports appears.

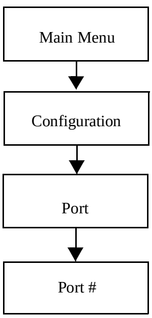
3. Select the port that you want to configure with the PPP protocol and enter that port's number in the **Enter port number** field.

NOTE: You must select a port that is capable of handling the dial PPP protocol. This is normally an asynchronous port. Any V.24 or X.21 interface can support async PPP. If you want to configure multilink PPP, you must use an ISDN port. (See Chapter 9 for ISDN configuration.)

✓ A menu showing the port parameters that are currently set for the port appears.

4. If the port is not currently configured as PPP, toggle the **Port type** field until **PPP** or **Async PPP** appears and press **<tab>**.

✓ The screen displays the parameters that need to be configured for the PPP line, as shown in Figure 10-4. These parameters are described in Table 10-2.




```
                    ***PPP Asynchronous Port Configuration***
Port:  3  IS-35                                     Last changed:  6-5-02  11:26:45

 |---  Press <RET> to toggle values  --||--- Type in values.  Max chars shown in ()  ---|
Port type:       Async PPP       Port name:       Sync/Async                        (14)

Connection mode:        DIAL               (Note: Configure entries in PPP Dial Directory)

Modem speed:            19.2 kbps
Calls supported:        Dial-in & out
Modem signaling:        AT
Modem command:          AT&FE0Q0V1&D2&C1&Q1S0=1                                     (35)


          For incoming calls
          Remote IP address          0.0.0.0
          Remote IPX address         0000000                                    (8 HEX)

          Authenticate remote with PAP: N              CHAP: N
          Local PAP/CHAP ID:                                                 (32 ASCII)


________[DynaStar_3614]_________                Process selections (Y/N): Y
 Use TAB & CURSOR keys to move among fields.   Press ESC to abort command & exit.
```

Figure 10-4 Asynchronous PPP Port Configuration Screen

5. In the **Port name** field, enter a name that will help you identify this port. This name will subsequently appear in any list of the ports, such as the list from which you select a port to configure.

6. Enter **Dial** as the connection mode for this line. **Dial** means that the port is a physical DTE and is used for dial connections. (For a DCE or DTE connection, see *Dedicated PPP Line Configuration* above.)

   NOTE: If you intend to configure a dial line on a synchronous connection, the attached modem must be able to support synchronous protocols.

7. Select the modem speed.

8. In the **Calls supported** field, indicate whether incoming and/or outgoing calls will be allowed.

9. If you are using a dial modem connection, retain modem signalling as **AT** and set the modem to Auto-answer on the first or second ring.

10. Indicate the modem command that should be used. The default command provides generally acceptable values.

11. Enter the IP and IPX addresses for the remote client in the **Remote IP/IPX address** fields.

12. Indicate the use of PAP or CHAP in the appropriate fields. (See the section *PPP Authentication* later in this chapter for more information.)

13. In the **Process selections** field, enter **Y** and press **<return>**.

14. You must complete your dial configuration by configuring your dial destinations in the PPP Dial Directory screen as described in the next section, *Configuring the PPP Dial Directory.*

15. To complete your configuration for an IP connection, you may need to configure static routes. See Chapter 12, *The IP/IPX Router Application*.

Table 10-2 Dial PPP Port Parameters

Parameter	Description	Values
Port type	The type of traffic the port will handle. **<return>** toggles through permissible values. A menu specific to the type selected appears when the cursor is moved from the field.	Depends on line type
Port name	A name to help you identify this port.	Max 14 chars
Connection mode	The physical level connection of the port. Dial means that the port is a physical DTE used for dial connections. See Table 10-1 for information on DTE and DCE lines.	Dial DTE DCE

Table 10-2 Dial PPP Port Parameters (cont.)

Parameter	Description	Values
Modem speed	The speed of the connected modem.	Normal sync/async: 9.6 kbps, 19.2 kbps, 38.4 kbps, 56.0 kbps, 64.0 kbps, 128.0 kbps For ISDN: 112 kbps data, 112 kbps voice 128 kbps data
Calls supported	Indicates whether the line will accept incoming only calls, outgoing only calls, or both incoming and outgoing calls.	Dial-in & out =default Dial-in only Dial-out only
Modem signaling	Indicates whether the AT command set is supported or V.25 bis. For async PPP, select AT.	AT=default V25bis
Modem command	The command to be sent to the modem when Modem signaling is set to AT. A generally acceptable command is given as the default. You can change this to suit your particular modem.	Standard AT modem command
Remote IP address	The address of the remote IP client.	Standard IP address Default=null
Remote IPX address	The address of the remote IPX client.	8 HEX digits Default=null
Authenticate remote with PAP/CHAP	Indicates whether PAP/CHAP authentication will be used to determine if the remote end is a valid user. See the section *PPP Authentication* later in this chapter for more information.	Y N=default
Local PAP/CHAP ID	Defines the local PAP/CHAP identification if the local unit is required to provide this information. See the section *PPP Authentication* later in this chapter for more information.	Max 32 chars Default=null

ADDRESS ASSIGNMENT. Incoming PPP calls can be assigned a fixed IP address (configured on a port-by-port basis) or a unique IP address from a pool of addresses so that no two concurrent calls have the same address.

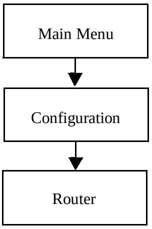
To configure this pool:

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) appears.

2. From the Configuration Comands menu, select **Router**.

✓ The Router Commands menu (Figure 10-5) appears.

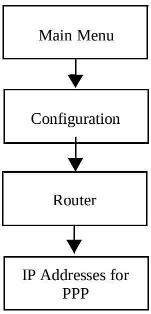



```
                    *** Router Commands***

      1 - IPX port information
      2 - IPX RIP & SAP settings
      3 - IPX RIP static routes
      4 - IPX SAP static routes
      5 - IP port information
      6 - IP static routes
      7 - IP application routing
      8 - OSI Static Routes
      9 - OSPF Global Information
     10 - OSPF Area Information
     11 - OSPF Port Information
     12 - OSPF Range Information
     13 - OSPF Virtual Link Information
     14 - IP Addresses for PPP
     15 - BOOTP Server Information
     16 - OSI/IP Tunnel Routes

 ________[DynaStar_3614]_________
Terminate input with <RET>.            Press ESC to return to previous menu.
```

Figure 10-5 Router Commands Menu

3. Select **IP Addresses for PPP**.

✓ The PPP IP Address Configuration screen (Figure 10-6) appears.




```
***PPP IP Address Configuration***
                                          Last changed:  6-7-02 11:26:45

Base IP Address:    0.0.0.0
Number of Users:   0                         (255 Max)

________[DynaStar_3614]_________                    Process selections (Y/N): Y
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit
```

Figure 10-6   PPP IP Address Configuration Screen

4. Enter the IP address in the **Base IP Address** field and enter the number of users allowed to use this address. If this number is exceeded, additional calls using this address will be cleared.
5. In the **Process selections** field, enter **Y <return>**.

■ Configuring the PPP Dial Directory

Parameters for dial destinations are configured on the PPP Dial Directory menu. On this menu, you also assign a location name as an identifier for the destination. This name will then be displayed on the Dial Directory and Call Control menus. Before you can configure the dial entries, you must first have configured a port to handle the PPP protocol, as explained in the previous section of this chapter.

To configure dial directory entries:

1. From the Main menu, select **Configuration**.

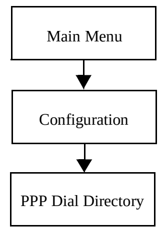
✓ The Configuration Commands menu is displayed.

2. Select **PPP Dial Directory**.

✓ The PPP Dial Directory Location Names screen is displayed. If no previous entries have been configured in the directory, the screen will look like the one in Figure 10-7. If there already are entries, the screen will resemble the one in Figure 10-8. The parameters in this screen are explained in Table 10-5.

```
                  ***PPP Dial Directory Location Names***
                                              Last changed:  6-7-02 11:26:45





                          Enter location number:

 ________[DynaStar_3614]_________
To add entry, just press <RET>.            Press ESC to return to previous menu.
To edit entry, enter loc # <RET>.                    Press UP/DOWN to scroll.
To delete entry, enter loc # <CNTL-D>.      NOTE:  Delete takes place immediately.
```

Figure 10-7 PPP Dial Directory Screen with No Previous Entries



```
                  ***PPP Dial Directory Location Names***
                                              Last changed:  6-7-02  11:26:45

# Location Name     IP    IPX    B     C     ML    PR    PL    CR    CL

1: Atlanta          Y     N      N     Y     N     N     N     N     N
2: Tallahassee      Y     N      N     Y     N     N     N     N     N
3: Burbank          Y     N      N     Y     N     N     N     N     N
4: Washington       Y     N      N     Y     N     N     N     N     N
5: Seattle          Y     N      N     Y     N     N     N     N     N




                          Enter location number:

________[DynaStar_3614]_________
To add entry, just press <RET>.            Press ESC to return to previous menu.
To edit entry, enter loc # <RET>.                     Use UP/DOWN to scroll.
To delete entry, enter loc # <CNTL-D>.    NOTE: Delete takes place immediately.
```

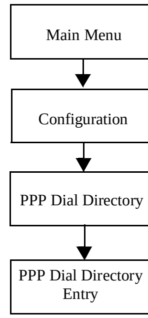
Figure 10-8 PPP Dial Directory with List of Available PPP Dial Locations

3. To configure a new entry, press **<return>**.
OR
To modify an existing entry, enter the appropriate location number in the **Enter location number** field and press **<return>**.

✓ A screen similar to Figure 10-9 is displayed. For a new entry, the screen contains default parameters. If you are modifying an existing entry, the screen contains the current parameters for that location.

```
***PPP Dial Directory Entry***

| --Press <RET> to toggle values. --|  | –Type in values. Max chars shown in ( ) --|

                                        Location name:                        (17)
Dialing type:      ISDN                 ISDN Interface: 100-Trunk 1/1
Call data rate:  56 kbps data           Phone Number:                         (21)

Authenticate remote with PAP:   N       CHAP:    N
Local PAP/CHAP ID:                                                      (32 ASCII)

Traffic type permitted on call
     IP Routing:            Y              Remote IP address:  0.0.0.0
     Ethernet Bridging:     N              Local IP address:  0.0.0.0
                                           Local Mask address:  0.0.0.0
     IPX Routing:           N
Compression:                N

IP Routing Protocol:          NONE
Use as default IP route:      N

________[DynaStar_3614]_________                Process selections (Y/N): Y
Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields.  Press ESC to abort command & exit.
```

Figure 10-9   PPP Dial Directory Entry



4. Enter a **Location name** that will help you identify the call destination.

✓ Once you process the entry, the **Location name** will be listed in the PPP Dial Directory.

5. Select the **Dialing type**.

> **NOTE:** For multilink PPP, you must select **ISDN**. For asynchronous PPP, select **AT Async**, and for synchronous PPP, select **AT Sync**.

6. Select the data rate for the call.

> **NOTE:** For standard synchronous or asynchronous PPP, select from 9.6 - 128 kbps. If you have selected **ISDN** as the dialing type, you can select from data rates that will use the multilink feature: 112 kbps data, which establishes two 56 kbps data channels; 112 kbps voice, which establishes two 56 kbps voice channels when the service provider makes a distinction between voice

and data; and 128 kbps data, which establishes two 64 kbps data channels.

✓ If you have selected a multilink PPP data rate, a new field, **Inv Mux phone**, appears to the right.

7. In the **Phone Number** field, enter the phone number that you will use to reach this destination.

8. For multilink PPP, fill in the phone number to be used for the second B-channel in the **Inv Mux phone** field. This can be the same number as in the **Phone Number** field if you are implementing a hunt group.

9. If you are using PAP and CHAP, fill in the related fields as required. (See *PPP Authentication* later in this chapter for more information on PAP and CHAP.)

10. Select the types of traffic that the call will support: **IP Routing**, **IPX Routing**, or **Ethernet Bridging**.

NOTE: These settings override the settings on the port configuration menu.

✓ If you enable **IP routing**, the fields **Remote IP address**, **Local IP address**, and **Local Mask address** are displayed to the right, and two new fields appear at the bottom of the menu: **IP routing protocol** and **Use as default IP route**.

✓ If you enable **IPX routing**, the field **Novell network number** is displayed to the right. A new field also appears at the bottom of the menu: **Use as default IPX route**.

11. In the **Compression** field, specify whether compression is to be used.

NOTE: Compression is most effective on lines operating at lower speeds and used for transferring text files. When compression is used, the devices at each end of the PPP link must support the LZS Compression protocol. *DYNASTAR* products with software version 4.01 and later support this protocol.

12. For IP configuration, fill in the IP address.

13. If IP routing is enabled, select the **IP Routing Protocol**: **NONE**, **RIP**, or **RIP II**.

14. If IP or IPX routing is enabled, specify whether the connection will serve as the default IP or IPX route.

15. If you have not specified this as the default IPX route, fill in the **Novell network number** on the right of the screen.

16. When your selections are complete, enter **Y** in the **Process Selections** field and press **<return>**.

✓ The top level PPP Dial Directory screen (Figure 10-8) is displayed. The location name you supplied is listed.

17. Configure the systemwide PPP dial parameters, as explained in the next section, *Systemwide PPP Parameters*.

18. If required, complete the IP routing configuration as explained in Chapter 12, *The IP/IPX Router Application*. (You must configure static routes if you selected **NONE** for the **IP Routing Protocol** in step 13.)

Table 10-3 Dial PPP Directory Parameter Values

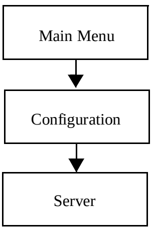
Parameter	**Description**	**Values**
Location name	The destination of this call.	17 chars max Default=null
Dialing type	For multilink PPP, select ISDN. For asynchronous PPP, select AT Async, and for synchronous PPP, select AT Sync.	ISDN AT Async AT Sync
Call data rate	The speed of the call. For standard synchronous or asynchronous PPP, select from 9.6 - 128 kbps. If you are using multilink PPP, select from 112 kbps data (two 56 kbps data channels); 112 kbps voice (two 56 kbps voice channels); or 128 kbps data (two 64 kbps data channels).	Depends on dialing type

Table 10-3 Dial PPP Directory Parameter Values (cont.)

Parameter	Description	Values
ISDN Interface	Indicates which ISDN line will be used for the outgoing call. The default is the lowest numbered D-channel.	2 - D Channel 100 - Trunk 1/1 150 - Trunk 1/2
Phone Number	The destination phone number to dial.	Max 19 digits Default=null
Inv Mux phone	Appears only if ISDN multilink is configured. Indicates the phone number for the second B-channel to call. Can be the same number as above if the number is part of a hunt group.	Max 19 digits Default=null
Authenticate remote with PAP/CHAP	Indicates whether PAP/CHAP authentication will be used to determine if the remote end is a valid user. See the section *PPP Authentication* later in this chapter for more information.	Y N=default
Local PAP/CHAP ID	Defines the local PAP/CHAP identification if the local unit is required to provide this information. See the section *PPP Authentication* later in this chapter for more information.	Max 32 chars Default=null
Traffic type permitted on call	Indicates which types of traffic (IP, IPX, Bridged) will be permitted on this connection.	Y N
Remote IP Address	Destination IP address	Valid IP address Default=0.0.0.0
Local IP Address	IP address used to identify the PPP connection on this *DYNASTAR*	Valid IP address Default=0.0.0.0
Local Mask address	Mask, if any, for the local IP address	Valid IP address Default=0.0.0.0
IP address	Appears only when IP Routing is set to Y. Indicates the destination IP address.	Valid IP address Default=0.0.0.0

Table 10-3 Dial PPP Directory Parameter Values (cont.)

Parameter	Description	Values
Novell network number	Appears only when IPX Routing is set to Y. Indicates a logical IPX network formed by the two PPP ports used in the call (this is the next hop for the call). Must be filled in if Use as default IPX route is set to N.	8 hex chars
Compression	Indicates whether compression will be used for the IP traffic on this line. To use compression, you must enable LZS Link Compression in the Applications menu under System Functions.	N=default Y
IP Routing Protocol	If NONE is selected, you must also set up IP static routes (see Chapter 12, *The IP/IPX Router Application*). Selecting NONE may help on large networks when routing over low-speed WAN links is required, as it keeps the routers from exchanging routing information packets over the link. Use RIP II if there is a *DYNASTAR* on each end of the link.	NONE RIP RIP II
Use as default IP/IPX route	If you select Y for this parameter, this connection will forward all IP/IPX traffic unless a more efficient path (with a lower tick count) is available.	Y N



■ Configuring Systemwide PPP Parameters

The Systemwide Parameters screen contains several parameters that define idle timers for PPP dial calls. These parameters are the first four timer parameters in the screen, as shown in Figure 10-10

```
                        *** Systemwide Parameters***


Server name: DynaStar399c                                                   (47)
Supervisor console herald:     DynaStar Supervisor                          (32)
Dial IP idle timer:            2              (0-disable, 1-254 min, 255-10 sec)
Dial IPX idle timer:           2                          (0-disable, 1-255 min)
Dial Bridge idle timer:        2                          (0-disable, 1-255 min)
B Channel call timeout:        0                         (0-disable, 1-1440 min)
X.25 call set-up timer:        5                                      (1-30 min)
XOT Idle Timer                 0                           (0-disable, 1-30 min)
PPP IP prioritization:         0                             (0 - disable, 1-99)
IPX-In preferred File Server:                                               (47)
IPX-Out broadcast address:     399c                                          (8)
Reserved LCNs:                 N                                  <CR> to toggle
Exhaustive Routing:            ENDPOINT                           <CR> to toggle
x32 No LCN Drop Timer:         6                       <0-disable, 1-12<10 sec>>
Daughter Board Auto-Recover:   Y                                  <CR> to toggle



_______[DynaStar 399c]_______                      Process selections (Y/N): Y
Use <TAB> and CURSOR to move fields.   Press ESC to return to previous menu
```

Figure 10-10 Systemwide Parameters Screen

These parameters cause PPP connections to disconnect when no traffic is detected for a specified amount of time. The **B Channel call timeout** parameter causes the BRI interface (both B-channels and the D-channel) to be disabled. Once disabled, no incoming or outgoing ISDN calls can take place until the D-channel is reenabled.

The idle timers (**Dial IP**, **Dial IPX**, and **Dial Bridge** traffic) simply cause the line to be disconnected. These three timers apply to all dialed PPP connections.

The idle timers are active only if the NCP layer has been negotiated. For instance, if the IP timer is set to 1 but the IP

NCP layer has not been enabled, the line will not be disconnected if there is no IP traffic for over 1 minute.

All active timers must expire for the connection to be disconnected. For example, if the IP and IPX timers are both active and set to 1, and there is no IPX traffic but there is IP traffic every 30 seconds, then the line will not be disconnected.

Setting an idle timer to 0 disables the timer. If an NCP layer is up and the corresponding idle timer is set to 0, the link will never be disconnected regardless of how the other idle timers are set.

The following types of traffic do not prevent idle timer or call timeouts:

- All outgoing traffic
- Traffic before the NCP layer is up
- IP broadcasts
- IPX broadcasts
- IPX packets where source or destination sockets are not equal to 0x451

Both the calling and called ends of the connection maintain these times and can disconnect the links.

■ PLACING A PPP DIAL CALL

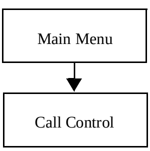
Although many dial-up connections are placed automatically when a remote service is required by an application, calls can be placed manually by selecting a destination from the PPP location names you previously configured.

CAUTION: Please be aware of how dial calls will be initiated and disconnected in your dial environment to avoid unnecessary phone charges.

To set up a call manually:

1. From the Main menu, select **Call Control**.

✓ The Call Control Commands menu, as shown in Figure 10-11, is displayed.




```
                        ***Call Control Commands***


    1 - Call status/disconnect     Check call status and manually disconnect calls
    2 - Manual call setup          Select location to call
    3 - X.25 Connections           Check X.25 Call Status
    4 - User call status           Check connected users
    5 - TCP connections            Check TCP connection status



                         Enter command number:

 ________[DynaStar_3614]_________
Terminate input with <RET>.              Press ESC to return to previous menu.
```

Figure 10-11 Call Control Menu

2. Select **Manual call setup**.

✓ The PPP Dial Directory Location Names screen (Figure 10-12) is displayed.

PPP Dial Directory Location Names

Last changed: 3-25-02 11:26:45

# Location Name	IP	IPX	B	C	ML	PR	PL	CR	CL
1: Atlanta	Y	N	N	Y	N	N	N	N	N
2: Tallahassee	Y	N	N	Y	N	N	N	N	N
3: Burbank	Y	N	N	Y	N	N	N	N	N
4: Washington	Y	N	N	Y	N	N	N	N	N
5: Seattle	Y	N	N	Y	N	N	N	N	N

Enter location number to call:

________[DynaStar_3614]_________

Press ESC to return to previous menu.

Figure 10-12 PPP Dial Directory Screen for Placing a Call

3. From the list, find the location that you want to call.
4. Enter the number of the location in the field **Enter location number to call** and press **<return>**.

✓ A connection is attempted. The Call Status/Disconnect screen (Figure 10-13) appears, displaying the status of your call. For more details on this screen, see the section *Monitoring Dial Connections* in Chapter 19, *Monitoring and Statistics*.

DISCONNECTING CALLS

Dial-up calls, including bridge calls, are disconnected after a period of inactivity on the link, as specified by the idle timer settings on the Systemwide Parameters menu. However, there may be instances when you want to disconnect a call manually.

NOTE: Dedicated calls are typically not disconnected while the *DynaStar* is powered on. If you need to take down a dedicated call from the *DynaStar*, do not use this procedure. Instead, disable the port (see Chapter 4, *System Functions and Parameters*.)

To disconnect an active call manually:

1. From the Main menu, select **Call Control**.

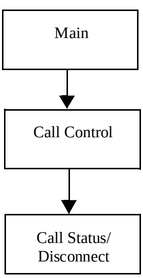
✓ The Call Control Commands menu (Figure 10-11) is displayed.

2. Select **Call status/disconnect**.

✓ The Call Status/Disconnect menu (Figure 10-13) is displayed.

3. Enter the port number to be disconnected in the field provided and press **<return>**.

✓ The call is cleared.



***Call Status/Disconnect**

Port	Interface	Type	Speed	Called number	Call Progress	Last Call duration dd/hh/mm/ss	Clear Cause
3	B Channel 2	PPP	64k	7035553007	Connected	00:13:45	
4	B Channel 1	PPP	64k	7035553007	Idle	00:02:13	-16
101	B Channel 7	PPP	64k	7035553009	Connected	00:07:14	

To disconnect a call, enter port number:

________[DynaStar_3614]_________

Press <RET> for statistics update. Press UP/DOWN to scroll.

Press <CTRL-D> to clear statistics. Press ESC to return to previous menu.

Figure 10-13 ISDN Call Status/Disconnect Screen

■ PPP AUTHENTICATION

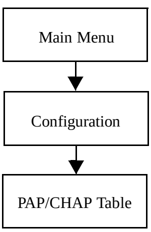
PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) are both authentication mechanisms that can be negotiated as part of the Link Control Protocol (LCP) on a PPP link to identify the remote end. By default, authentication is not required on a PPP link. However, authentication is frequently used to ensure that only valid users are gaining access to network resources. It is possible for one party to ask for authentication with PAP and for the other party to ask for authentication using CHAP.

PAP security is based on a shared password that is transmitted over the line. The party that is asked to authenticate itself sends its ID and password to the other side, which compares them to its table of valid IDs and passwords. However, because the ID and password are sent in the clear, they are vulnerable to eavesdropping.

CHAP security is based on a shared “secret” that is configured in both units but is never transmitted. The party that is asked to authenticate itself is sent a randomly derived challenge, to which it provides a response that contains an ID and a value derived from the challenge data and the “secret” value that is shared by the two parties. Since this response changes with each request, an eavesdropper will not be able to provide a valid response at the next authentication request.

If PAP or CHAP is requested, the higher layers are not configured until the authentication is successful. With CHAP, a challenge can be issued at any time, even after the higher layers have been configured. The *DYNASTAR* will respond to challenges at any time, but it will issue a challenge only once after the link layer has been configured.

PAP/CHAP VALUES TABLE. The PAP and CHAP values are configured from the PAP/CHAP Values screen (Figure 10-14), which is accessed from the Configuration Commands menu. The entries on this screen are used both to authenticate remote units and to provide authentication of the local unit with remote units (parameters are explained in Table 10-4). To set up PAP or CHAP authentication, you must also configure fields in the PPP Port Configuration screen or the PPP Dial Directory screen, as described in the earlier sections of this chapter.




```
                              ***PAP/CHAP Values***
                                         Last changed: 4-23-02  22:06:56

01:  ID:                                                 (32 ASCII)
     PW:                                                 (32 ASCII)
     Secret:                                             (32 ASCII)
     Scope   Port:          Tel#:                        (12 NUMBER)
02:  ID:                                                 (32 ASCII)
     PW:                                                 (32 ASCII)
     Secret:                                             (32 ASCII)
     Scope   Port:          Tel#:                        (12 NUMBER)
03:  ID:                                                 (32 ASCII)
     PW:                                                 (32 ASCII)
     Secret:                                             (32 ASCII)
     Scope   Port:          Tel#:                        (12 NUMBER)
04:  ID:                                                 (32 ASCII)
     PW:                                                 (32 ASCII)
     Secret:                                             (32 ASCII)
     Scope   Port:          Tel#:                        (12 NUMBER)

                                             Process selections (Y/N): Y

In left most field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.   Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 10-14 PAP/CHAP Values Screen

Table 10-4 PAP/CHAP Screen Parameters

Parameter	Description
ID	This field is mandatory for each entry. It provides an identification that can be used to identify a remote unit or the local unit.
PW	The password to be passed for PAP authentication.
Secret	The secret value to be used for CHAP authentication.
(Scope) Port	If a port number is entered, the entry can be used for authentication of units attached to this port only. A port number of 255 indicates that this entry is for local identification only and will be provided in response to a remote's request for authentication.
(Scope) Tel#	Limits the authentication to a specific ISDN calling party.

The **ID**, **PW**, and **Secret** fields accept up to 32 alphanumeric characters. *The fields are case sensitive*. If an ID has both a password and secret defined for it, then it can be used for PAP or CHAP, depending on how the port is configured. (See *Port Configuration*, which follows.) If both the **PW** and **Secret** fields are blank, the ID can be used for PAP authentication and the password will be blank.

10

The PPP Application

PORT CONFIGURATION. Two fields also need to be configured in the port configuration screen. This can be the PPP Dial Directory Entry screen or the PPP Port Configuration screen, depending on what type of port you are configuring. The first field is **Authenticate remote with PAP/CHAP**. If PAP *or* CHAP is set to **Y** and a call uses this port, the *DYNASTAR* requires the remote party to authenticate itself using the specified method. If *both* PAP and CHAP are set to **Y**, the *DYNASTAR* first tries to use CHAP since it is more secure. If the remote unit does not support CHAP, the local unit then attempts to use PAP.

The second field is **Local PAP/CHAP ID**. If a value is entered here, the *DYNASTAR* can authenticate itself if so requested by the remote party. The ID here must match an entry in the PAP/CHAP Values table.

EXAMPLE. This section explains the configuration of the scenario illustrated in Figure 10-15.

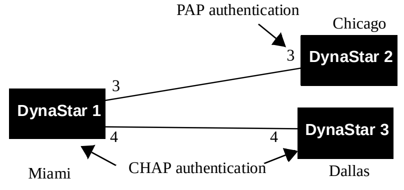


Figure 10-15 PAP/CHAP Configuration Example

In this example, the Chicago *DYNASTAR* initiates a PPP call to Miami that comes in on port 3. Miami wishes to use PAP to authenticate this call. The *DYNASTAR* in Dallas calls from its port 4 to Miami port 4; in this case, both ends want to verify the remote using CHAP authentication.

Configuration of Miami *DYNASTAR*

*** Remote PAP/CHAP Values ***

[Configure the remote PAP authentication for port 3]

1. ID: DS100Chicago3		[ID of remote unit]
PW: LakeMichigan		[PAP password]
Secret:		[For CHAP, so not needed here]
Scope Port:	Tel#:	[Not limited to any port]

[Configure the remote CHAP authentication for port 4]

2. ID: DS100Dallas4 [ID of remote unit]
   PW: [For PAP, so not needed here]
   Secret: FortWorth [CHAP secret]
   Scope Port: 4 Tel#: [Limits use to port 4 only]

[Configure the local CHAP authentication for port 4]

3. ID: DS100Miami4 [ID of local unit]
   PW: [For PAP, so not needed here]
   Secret: OCEAN [CHAP secret]
   Scope Port: 255 Tel#: [For local unit to authenticate itself only; will not be used to authenticate a remote.]

Configuration ofPAP/CHAP fields in the PPP port configuration screens:

PORT 3:
Authenticate remote with PAP: Y CHAP: N
[Toggle to select the values.]
Local PAP/CHAP ID: [Null, since the remote end is not being set up to authenticate this port.]

PORT 4:
Authenticate remote with PAP: N CHAP: Y
Local PAP/CHAP ID: DS100Miami4
[A value is entered since this port is expected to provide authentication to the remote end.]

Configuration of Chicago *DYNASTAR*

*** Remote PAP/CHAP Values ***

[Configure the local PAP authentication]

1. ID: DS100Chicago3 [ID of this unit]
   PW: LakeMichigan [PAP password]
   Secret: [For CHAP, so not needed here]
   Scope Port: 255 Tel#: [Indicates local use only; will be used to verify an authentication request]

Configuration ofPAP/CHAP fields for the PPP port configuration screens:

PORT 3:
Authenticate remote with PAP: N CHAP: N
Local PAP/CHAP ID: DS100Chicago3
[A value is entered since this port is expected to provide authentication to the remote end.]

Configuration of Dallas *DYNASTAR*
[Configure the local CHAP authentication]

2. ID: DS100Dallas4	[ID of this unit]
PW:	[For PAP, so not needed here]
Secret: Fort Worth	[CHAP secret]
Scope Port: 255 Tel#:	[Indicates local use only; will be used to verify an authentication request]

[Configure the remote CHAP authentication for port 4]

3. ID: DS100Miami4	[ID of remote unit]
PW:	[For PAP, so not needed here]
Secret: OCEAN	[CHAP secret]
Scope Port: 4 Tel#:	[Use for port 4 only]

Configuration ofPAP/CHAP fields for the PPP port configuration screens:

PORT 4:
Authenticate remote with PAP: N CHAP: Y
Local PAP/CHAP ID: DS100Dallas4
[A value is entered since this port is expected to provide authentication to the remote end.]

PPP ENTRY CONFIGURATIONS. The PPP Dial Directory Location Names screen (Figure 10-9) displays a summary of the dial PPP entries. This summary indicates what features, including authentication, have been enabled when **Y** is listed in the corresponding column. The information on this screen is explained in Table 10-5.

Table 10-5 Dial PPP Entries

Mnemonic	Meaning
IP	IP routing is enabled.
IPX	IPX routing is enabled.
B	Bridging is enabled.
C	Compression is enabled.
ML	Multilink is enabled.
PR	PAP authentication of remote is enabled.
PL	PAP authentication of local is enabled.
CR	CHAP authentication of remote is enabled.
CL	CHAP authentication of local is enabled.

If the **Local PAP/CHAP ID** field contains an ID that does not have a corresponding entry in the PAP/CHAP table, then **PL** and **CL** will be set to **N**.

THE CSU/DSU MODULE

■ OVERVIEW

The *DYNASTAR 100e*, *DYNASTAR 2000*, *DYNASTAR 500*, and *DYNASTAR 5000* can act as a T1 or E1 CSU/DSU when the CSU/DSU module is installed. This capability is available only for ports 8 and 9 on the *DYNASTAR 500 /5000* and ports 4 and 5 on the *DYNASTAR 100e*/*2000*. For configuration purposes, ports 8 and 9 (or 4 and 5) are considered channels 1 and 2, respectively. "Virtual" ports 11 and 12 are considered trunks 1 and 2, respectively, and are internally connected to the channels.

The module is available in four configurations. Two configurations have two framers, so both ports are T1 or E1. The other two configurations have a single framer, so one port is T1 or E1 and the other port is a standardWAN port. The configurations are listed below:

- Dual T1
- Dual E1
- One WAN port (port 4/8) + single T1 (port 5/9 and trunk 12)
- One WAN port (port 4/8) + single E1 (port 5/9 and trunk 12)

NOTE: If you are using the CSU/DSU module in a *DYNASTAR 500*, you must also install a contact module in slot 3 or slot 5.

The *DYNASTAR* can also support a 56K/64K DDS interface with an integral CSU/DSU. This is described in the section *DDS Interface* later in this chapter.

■ CONFIGURATION

There are two distinct steps in configuring the CSU capability. The first step consists of configuring the trunk (port 11 and/or 12), and the second step consists of configuring the channel (port 8 and/or 9 or port 4 and/or 5). This is similar to other T1/E1 configurations in the *DYNASTAR*.

In the CSU configuration, the trunk can be assigned one of three modes:

- Single channel mode
- Single channel mode - drop and insert
- Dual channel mode - drop and insert

These three trunk types are described below.

SINGLE CHANNEL MODE

In single channel mode, the two “trunk” ports (11 and 12) operate totally independently of each other. This is illustrated in Figure 11-1.

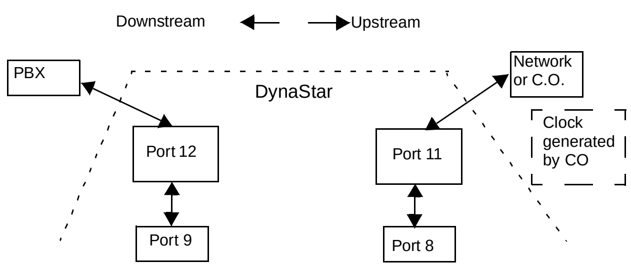


Figure 11-1 CSU Single Channel Mode

SINGLE CHANNEL MODE - DROP AND INSERT

In single channel mode/drop and insert, all unused time slots are transparently passed upstream and downstream. Port 8 terminates a time slot in the upstream direction, and port 9 terminates a time slot in the downstream direction. This mode can be used in a filtering application where a time

slot is terminated and only those calls that are allowed continue downstream and/or upstream. This is illustrated in Figure 11-2.

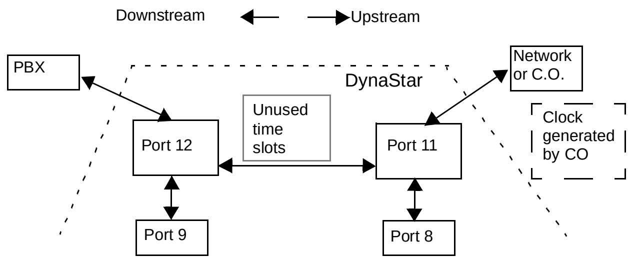


Figure 11-2 Single Channel Mode - Drop and Insert

Two Channel Mode - Drop and Insert

Two channel mode/drop and insert allows both ports 8 and 9 to terminate two separate applications on a single trunk (for example, port 11). The other trunk (port 12, if used) has all of the unused time slots transparently passed to it from the upstream trunk (port 11). This is illustrated in Figure 11-3.

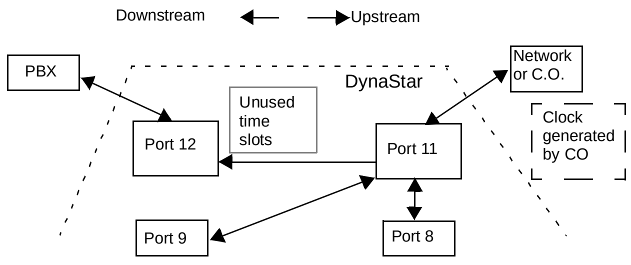


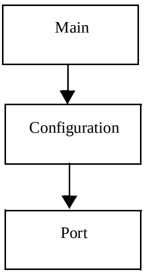
Figure 11-3 Two Channel Mode - Drop and Insert

TRUNK CONFIGURATION

To configure your CSU trunk:

1. From the Main menu, select **Configuration**.
2. From the Configuration menu, select **Port**.

✓ A Configure Port screen similar to the one in Figure 11-4 appears.




```
                         ***Configure Port***

Valid port numbers (with names) are:
     0: Ethernet
     1: 16-port card
     2: HS 8-port card
     3: QUAD card
     4: Dual T1/E1
     5: Contact
     6: Console
     7: Sync/Async
     8: CSU/DSU chan 1
     9: CSU/DSU chan 2
     10: Virtual PAD
     11: CSU/DSU trunk 1
     12: CSU/DSU trunk 2
     99: Virtual X.25 Ports
     400: Trunk 4/1
     450: Trunk 4/2
                                              Enter port number:

 ________[DynaStar_3614]_________
Terminate input with <RET>              Press ESC to return to previous menu
```

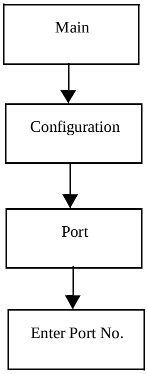
Figure 11-4 Configure Port Showing CSU/DSU Trunks and Channels

3. In the **Enter port number** field, enter the number of the first trunk you want to configure.

✓ The T1 Trunk Parameters screen (Figure 11-5) appears.

```
***T1 Trunk Parameters***

Port: 11                                  Last Changed: 4-23-02   23:45:00
Trunk Type:    Single channel             Trunk Name: CSU/DSU trunk 1(14)

Frame Type:    ESF                        Time Slot Bandwidth: 64 kbps
Line Coding:   B8ZS                       Yellow Alarm Mode: FDL
CRC 6:         On                         Line Build Out: 0 to 133 ft
                                          Transmit clk source: Trunk 1 Rx clk

-----------------------------------------Time Slot Assignments-----------------------------------------
01: 8     05: 8     09: --     13: --     17: --     21: --
02: 8     06: 8     10: --     14: --     18: --     22: --
03: 8     07: 8     11: --     15: --     19: --     23: --
04: 8     08: 8     12: --     16: --     20: --     24: --

   ________[DynaStar dc000345]________          Process selections (Y/N): Y
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 11-5 T1 (CSU/DSU) Trunk Parameters Screen



4. Select the **Trunk Type** to be either **Single Channel**, **Single Channel Drop and Insert**, or **Two Channel Drop and Insert**. The differences between these types were explained at the beginning of this section.

5. Select the **Transmit clk source** to be the trunk that is connected to the network—Trunk 1 (port 11) or Trunk 2 (port 12). The third possibility, Local Oscill, is for lab and standalone use only.

6. Complete the other parameters in the top portion of the screen as required by your network. Values should agree with the other end of the connection. See Table 9-2 for a description of all parameters and possible values.

7. In the Time Slot Assignments section of the screen, toggle to enter the channel that will be assigned to each time slot, or type in the channel number. The channel number can only be channel 8 (or 4) for port 11 and channel 9 (or 5) for port 12. The time slot assignment should match the assignment on the connected equipment.

8. When you have completed your configuration, type **Y** at the **Process selections** prompt to save and quit.

✓ You return to the Configure Port screen.

9. Repeat steps 1 through 8 to configure the other trunk, if required.

   NOTE: If you selected two channel - drop and insert as your type, there will be no time slots to assign on the second trunk.

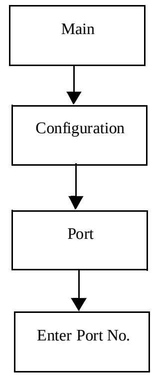
CHANNEL CONFIGURATION. You must now configure the parameters for the CSU/DSU channel to which you just assigned one or more time slots.

1. If you have just completed the trunk configuration in the previous procedure, press **ESC** once to return to the Configure Port screen (Figure 11-4).

2. Enter the number of the channel that you want to configure (for example, 8).

✓ The X.25 Port Configuration screen shown in Figure 11-6 appears.

NOTE: X.25 is the default protocol for these ports. A different configuration screen might appear if the port has been previously configured for a different protocol.




```
                    ***X.25 Port Configuration***
Port: TDM channel                          Last changed:  4-23-02  11:26:45

|- Press <RET> to toggle values. -|  |-Type in values. Max chars shown in () --|
Port type:              X.25 line            Port name:       CSU/DSU chan 1    (14)
                                             X.121 Address:                 (15 BCD)

Line speed:             448 kbps (8x56k)  Non-Zero DTE Cause:       N
Number of Flags:(0-15) 0                  Allow User Data:          Y
Calling address mod:   NONE               LAPB extended:            N
Local address insert:  N                  X.25 mode:                DTE
Max Window size:       7                  K LAPB window size:       7          (fixed)
Max Packet size:       1024               T1 Acknowledgment timer:  3     (1-255 sec)
Packet/Window Neg:     N                  T3 Idle timer:            30    (0-255 sec)
Require CUG:           N                  N2 Retransmission count:  20         (1-255)
Require NUI:           N                  N1 Max frame size:        8248 bits
Req Reverse Charging:N                    LCN Partition   Base LCN  Number of VCs
Route inbound calls on CUD: N                             (1-4095)
Traffic types permitted on line              Permanent:    1             0
        IP Routing:          Y               One-way in:   1             0
        IPX Routing:         Y               Two-way:      1             4095
        Ethernet Bridging:   Y               One-way out:  4095          0


________[DynaStar_3614]________                      Process selections (Y/N): Y
 Use TAB & CURSOR keys to move among fields.  Press ESC to abort command & exit.
```

Figure 11-6 Sample Configuration Screen for T1 Channel

3. Toggle the **Port Type** field until the protocol you want to define (PPP, X.25, HDLC, or frame relay) is displayed and press **<tab>** or an arrow key.

✓ The port configuration screen for the selected protocol appears.

NOTE: The fields in these screens are the same as those in the configuration screens for any port of this type, with the following exceptions: there is no Connection Mode field (DCE, DTE, Dial), and the line speed is calculated based on the time slots you assigned on the T1 Trunk Parameters screen.

For example, in Figure 11-6, the line speed shown is 448 kbps because eight 56k timeslots were assigned to Port 11 on the T1 Trunk Parameters screen (Figure 11-5). If the T1 trunk time slot bandwidth is set to **Either**, you can toggle between Nx56k and

Nx64k rates. Otherwise, the line speed cannot be changed.

4. Complete the parameters as required for your network. For additional information, see Chapter 6, *The X.25 Application*, Chapter 8, *The Frame Relay Application*, or Chapter 10, *The PPP Application*. (HDLC is discussed in Chapter 6.)

5. When you have completed the channel configuration, enter **Y** at the **Process Selections** prompt to save and exit.

✓ The Configure Port screen (Figure 11-4) appears.

6. Repeat steps 1 through 4 for port 9, if required.

■ DDS INTERFACE

Dataphone Digital Service (DDS) is a Bell System standard developed for delivering synchronous data over a dedicated 4-wire circuit. The *DYNASTAR* can be optioned to support 1 or 2 DDS interfaces, each with an integral CSU/DSU and a traditional RJ-48 interface. (See Appendix B for pin assignments.) The integral CSU/DSU supports network generated loopback modes for circuit testing.

Only the *DYNASTAR 100e* and *DYNASTAR 2000* support DDS. The physical interface resides in port 4 and/or port 5. Like the CSU/DSU configuration discussed earlier in this chapter, the configuration consists of two main steps: first configuring the trunk and then configuring the port.

DDS CONFIGURATION

1. From the Main menu, select **Configuration**.

2. From the Configuration menu, select **Port**.

✓ A Configure Port screen similar to the one in Figure 11-4 appears.

3. In the **Enter port number** field, enter the number of the first trunk you want to configure (This will be port 11 or 12.)

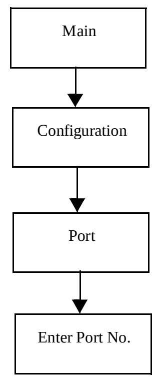
✓ The T1 Trunk Parameters screen (Figure 11-5) appears.

4. Toggle the **Trunk Type** to **DDS 56K/64K**.

✓ A screen similar to the one shown in Figure 11-7 appears.

```
                         ***DDS Trunk Parameters***

Port: 11                                      Last Changed: 4-23-02   23:45:00
Trunk Type:    DDS 56K/64K                    Trunk Name: CSU/DSU trunk 1(14)

Transmit clock source:      Receive Clock

Receiver gain (in dB):      AUTO

Receive threshold (dB):     AUTO

Remote Alarm Indication:    NONE




_______[DynaStar dc000345]_______            Process selections (Y/N): Y
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 11-7 DDS Trunk Parameters Screen



5. Configure the parameters as required. For most installations, you will not need to adjust the default parameters shown in Figure 11-7. Parameters and values are explained in Table 11-1.

6. When you have completed your configuration, enter **Y** at the **Process selections** prompt and press **<return>**.

7. You now need to configure the protocol for the port (4 or 5). These ports support several different protocols (such as frame relay, X.25, PPP, etc.). Refer to the appropriate section of this manual for details on configuring the different port types.

Table 11-1 DDS Parameters

Parameter	Description	Value
Trunk Name	A user configurable name to identify this trunk. Default name is “CSU/DUS trunk 1”.	Max. 14 alphanumeric characters
Transmit Clock Source	The transmit clock source. Local oscillator causes the *DYNASTAR* to use its internal clock for transmit timing.	Receive clock (default) Local oscillator
Receiver Gain	The receiver gain	Not configurable
Receive Threshold	The receive threshold. Toggle to various fixed values or Auto.	Auto (default) Various fixed values
Remote Alarm Indication	Indicates whether or not there will be remote alarm indication. DMI (Data Mode Idle) means that when the *DYNASTAR* detects a bad receive line condition, it will signal the remote end with a special alarm pattern.	None (default) DMI

THE IP/IPX ROUTER APPLICATION

12

INTRODUCTION

Every *DYNASTAR* is configured with IP/IPX router software that allows it to be connected to one or more Ethernet or LANs over synchronous or asynchronous lines. Traffic can be routed between Ethernet LANs, and IP and IPX traffic can be simultaneously transmitted on a connection between two routers.

The *DYNASTAR* can be connected to any other router that supports IP/IPX and the appropriate RFC protocols. All *DYNASTAR* connections can carry both bridge and router (Brouter) traffic. When the *DYNASTAR* is configured as a Brouter, IP/IPX traffic is automatically routed. All other traffic, such as DECnet, SNA, XNS, and OSI, is bridged.

The *DYNASTAR* IP/IPX router includes these features:

- Dial-on-demand IP and IPX routing whenever the *DYNASTAR* detects traffic for a remote network
- Support for static RIP, RIP-II, and OSPF routing
- RIP and SAP spoofing (for dedicated and dial connections)
- IPX-In and IPX-Out capability to allow asynchronous devices to connect to a Novell LAN and allow Novell Netware LAN users to access asynchronous devices
- Support for the SLIP protocol
- Ability to act as a BOOTP relay agent

The *DYNASTAR* supports connections between a pair of IP/IPX routers over any of the following:

- A leased line
- A switched circuit over an X.25 packet network
- A frame relay line

- A connection to a Point-to-Point (PPP) based network, using dial-up or dedicated synchronous or asynchronous lines (see Chapter 10, *The PPP Application*, for more information).

■ THE IP ROUTER

IP (Internet Protocol) is a protocol that allows devices to communicate over local area networks (LANs). The *DYNASTAR* IP router application lets LAN workstations access a distant IP host on any interconnected IP network. To access a distant IP host, the workstation user sends IP traffic to the host IP address. A typical IP configuration is shown in Figure 12-1.

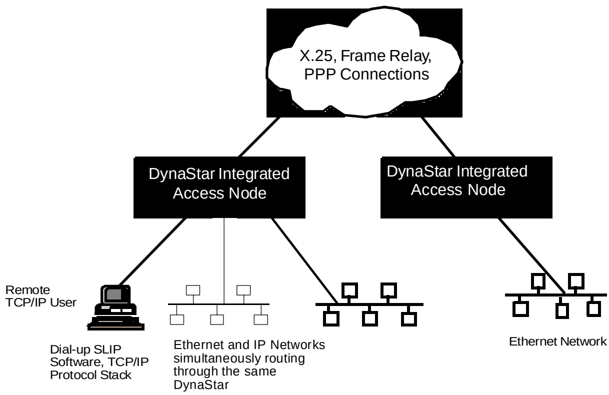


Figure 12-1 *DYNASTAR* Supporting an IP Router Application

Once configured, the *DYNASTAR* automatically forwards the IP frames to the distant IP network. To ensure that the IP host is reachable, the user can use the IP PING utility. PING permits the user to check that a path exists to each IP address along the route from the workstation to the IP host.

The command is entered on the *DYNASTAR* at thePAD prompt (*) in the following format:

ping <IP address>

If the device with the given IP address is properly connected, the *DYNASTAR* PAD displays a response in this format:

<IP address> is alive.

If the device is not connected or cannot be reached, an error response is displayed.

NOTE: The PAD prompt is accessible via physical connection of a dumb terminal, a Telnet connection to a virtual port, or an X.25 virtual connection to a virtual port. On the *DYNASTAR*, one or more ports must be configured with a valid IP address for the ping to work.

When an IP frame is destined for an IP network other than the local IP network, the IP frame is sent to the local *DYNASTAR*, which is serving as the IP router. If more than one IP router is present on the IP network, the IP router that receives the frame redirects the IP frame to the "best" router on the local IP network.

An IP routing protocol is required to forward IP frames from one IP network to another. The routing protocol automatically determines the best path to any other IP network. As an option, static routes to remote IP networks can be manually entered.

IP ADDRESSES

Every port carrying IP traffic must be identified with an IP address. IP addresses are 32 bits long and are written as four decimal numbers separated by periods (for example, 128.50.150.33). This is called "dotted decimal" notation. Each number represents 8 bits of the address.

The address is divided into two fields: a network number and a host number. The length of the network number and the host number is determined by the value of the first number in the address, as shown in Table 12-1, which shows the three possible classes of IP addresses.

Table 12-1 IP Address Classes

Class	Network number	Host number	Range of first digits
A	8 bits	24 bits	1-126*
B	16 bits	16 bits	128-191
C	24 bits	8 bits	192-223

* 127 is reserved for loopback testing.

The network address can be extended by allocating bits of the host address to a subnet. A 32-bit subnet mask must be specified for each IP address to identify the bits in the IP address that make up the network and subnet numbers. The mask is used to derive the remote IP network number by ANDing the mask with the IP address. The mask, like the IP address itself, is also written as four decimal digits (each representing 8 bits).

When a network is split into subnets, the network number identifies the *DYNASTAR*. Subnet addresses are used by the *DYNASTAR* to route traffic to local LAN interfaces.

You can obtain IP addresses from your network administrator or Internet service provider.

CONFIGURING AN IP CONNECTION

1. Set up the physical network connections and cabling.
2. Configure the correct protocol for the port you will be using.
    - For an X.25 port, see Chapter 6.
    - For a frame relay port, see Chapter 8.
    - For a PPP port, see Chapter 10.
3. Configure the routes as required for the port type you configured.

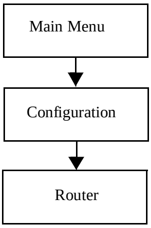
- For X.25, configure the X.25 Bridging and Routing table (see Chapter6).
- For frame relay, configure the DLCIs (see Chapter 8).
- For dial PPP, configure the PPP Dial Directory (see Chapter 10).

4. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) appears.

5. Select **Router**.

✓ The Router Commands menu appears, as shown in Figure 12-2.



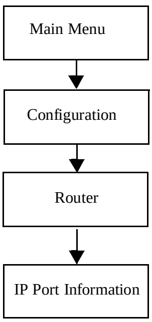

```
                    ***Router Commands***

 1 - IPX port information
 2 - IPX RIP & SAP settings
 3 - IPX RIP static routes
 4 - IPX SAP static routes
 5 - IP port information
 6 - IP static routes
 7 - IP application routing
 8 - OSI Static Routes
 9   - OSPF Global Information
10 - OSPF Area Information
11 - OSPF Port Information
12 - OSPF Range Information
13 - OSPF Virtual Link Information
14 - IP Addresses for PPP
15 - BOOTP Server Information
16 - OSI/IP tunnel Routes
17 - VPN Directory
                         Enter command number:

________[DynaStar_3614]_________
Terminate input with <RET>.          Press ESC to return to previous menu.
```

Figure 12-2 Router Commands Menu

6. Select **IP port information**.

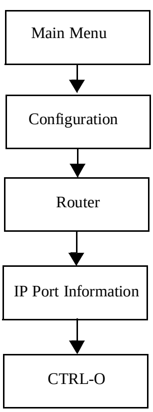
✓ The IP Port Information screen appears, as shown in Figure 12-3. The screen for modules with multiple lines is shown in Figure 12-4. (You reach this screen by navigating to the appropriate interface on the IP Port Information screen and entering **<CTRL-O>** .)

NOTE: The desired port must have IP cnabled on its port configuration screen.




```
                         ***IP Port Information***
                                              Last changed:  4-23-02  11:26:45

 Port        Interface          IP Address        IP Mask       |-- Use RET to toggle--|
                                  x.x.x.x         x.x.x.x           Protocol      Encaps
       0      Ethernet            100.1.1.1       255.0.0.0         RIP           Enet II
       7      Sync/Async          0.0.0.0         0.0.0.0           RIP
       8      HS WAN 1            0.0.0.0         0.0.0.0           RIP
       9      HS WAN 2            0.0.0.0         0.0.0.0           RIP
600 - 631     Virtual X.25        *

 ________[DynaStar_3614]_________               Process IP addresses (Y/N): Y
Lines with port ranges are multiport interfaces. Configure these ports together on one
line. Or with cursor on line, press <CTRL-O> to configure separately.
*Fields are blank on this screen if ports are configured separately.
```

Figure 12-3 IP Port Information Screen




```
                      ***IP Interface (1) QUAD Card***
                                              Last changed:  4-23-02  11:26:45
Port(s)          Interface         IP Address        IP Mask          |-- Use RET to toggle--|
                                     x.x.x.x         x.x.x.x          Protocol      Encaps
    102          QUAD102           0.0.0.0           0.0.0.0          RIP
    103          QUAD103           0.0.0.0           0.0.0.0          RIP
    104          QUAD104           0.0.0.0           0.0.0.0          RIP

________[DynaStar_3614]_________               Keep new IP Addresses (Y/N): Y
 You can configure each port of a multiport interface separately on this screen.
 Press ESC to return to previous screen.
```

Figure 12-4 IP Port Screen for Expansion Boards

7. Assign IP addresses to all ports that will be used for routing.

NOTE: All WAN or LAN ports to be used for routing must be assigned IP addresses on their own network. For more information on obtaining an IP address, see the previous section *IP Addresses*.

✓ Default IP masks appear for all ports to which you assigned an address. The mask is based on the address class.

8. If subnetting is to be used on a particular port, change the mask to specify the bits of the IP host number that are used for the subnet address.

9. Enter a routing protocol.

- **RIP** is the default standard IP routing protocol.
- Use **RIP II** if there is a *DYNASTAR* on both ends of the link.
- **NONE** keeps the routers from exchanging routing information packets over the link. This can be helpful on large networks that use low-speed WAN links, as it reduces the amount of traffic.

NOTE: Select NONE if you want to use static routing or OSPF routing protocol.

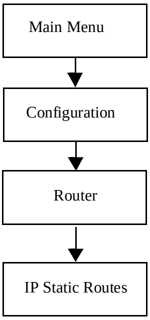
- **RIP-RX** specifies that RIP is only received and not transmitted. This reduces broadcast traffic.

10. To save your configuration and quit, enter **Y** in the **Process IP addresses** field and press **<return>**.

✓ You return to the Router Commands menu (Figure 12-2).

11. If you selected **NONE** in step 9, you must assign static routes. Continue with step 12 below.
If you do not need to assign static routes but want to configure filtering, see the next section, *IP Filtering*.

12. From the Router Commands menu, select **IP static routes**.



✓ The IP Static Routes screen appears, as shown in Figure 12-5.

```
                         ***IP Static Routes***
                                          Last changed:  4-23-02  11:26:45
          IP Address          IP Mask       Next Hop          Hops
          x.x.x.x             x.x.x.x       x.x.x.x           (0-15)
1:
2:
3:
4:
5:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:
Note: x = 0-255

 ________[DynaStar_3614]_________              Process Static Routes (Y/N): Y
In IP address field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.         Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 12-5 IP Static Routes Screen

NOTE: Up to 120 static routes can be configured.

13. In the **IP Address** column, enter the IP address of the remote network. Use zeros in the host octet position(s) (for example, 126.0.0.0 for a class A address, and 155.50.0.0 for a class B address, etc.).

NOTE: A static route of 0.0.0.0 can be used as a default route for routing any IP address that does not have a match in the routing table.

✓ A default mask appears.

14. If required, modify the IP mask for subnetting.

15. Under **Next Hop**, enter the IP address of the remote IP port used to access the IP network specified in this procedure. This can be:

- The IP address on a directly connected LAN

- The IP address at the remote end of the PPP link (as configured in the PPP Dial Directory screen)
- The IP address at the remote end of the X.25 virtual circuit (as configured in the Bridge and Router Call Addresses screen)
- The IP address at the remote end of the frame relay DLCI (as configured in the Bridge & Router & Switching DLCIs screen)
- The IP address at the remote end of the ATM connection (as configured in the VPI/VCI configuration screen)

16. In the **Hops** column, enter the number of hops to the remote network using this static route.

NOTE: If the number of hops entered here is greater than the number of hops in a dynamic route (using RIP) to the same IP network, then the dynamic route will be used.

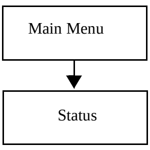
17. When you have completed your configuration, enter **Y** in the **Process static routes** field and press **<return>**.

18. If you want to configure filtering, see the section, *IP Filtering*.

CHECKING YOUR IP ADDRESSES. Once you have configured your IP addresses, you can verify your entries for all IP ports in the IP Addresses menu.

1. From the Main menu, select **Status**.

✓ The Status Commands menu, shown in Figure 12-6, appears.

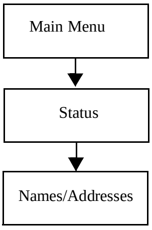



```
                    *** Status Commands ***

 1 - Board Status         Display internal module types and status
 2 - Call status          Check call status and manually disconnect calls
 3 - Names/Addresses      Verify names & MAC, IP, IPX and X.121 addresses
 4 - Statistics           Show statistics for port n
 5 - Buffer Usage         System buffer usage
 6 - Disable Port         Put port n in Disabled state (busy out dial ports)
 7 - Enable Port          Bring port n to an Enabled state
 8 - Initialize Port      Perform initialization on port n
 9 - Log                  Display system error log
10 - Monitoring           Show input/output data packets for port n
11 - Busy/UnBusy Port     Bring port n to Busy/UnBusy state
12 - PPP status           Check call status
13 - OSI                  OSI operator console
14 - Modem Status         Show statistics & status for modem resources
15 - Call History         Show status of transactions per ISDN port
16 - Trace                SNA Trace

                    Enter command number:

_________[DynaStar_3df2]__________
Terminate input with <RET>.            Press ESC to return to previous menu.
```

Figure 12-6 Status Commands Menu

2. Select **Names/ Addresses**.

✓ The Verify Names & Addresses Commands screen, shown in Figure 12-7, appears.




```
             ***Verify Names & Addresses Commands***

             1 - Port addresses  (MAC, IPX, IP, X.121)
             2 - IPX addresses
             3 - IP addresses
             4 - Port names
             5 - IPX-Out Service names
             6 - OSI routes
             7 - X.25 routes
             8 - X.25 routing Test

________[DynaStar_3614]_________
Terminate input with <RET>.            Press ESC to return to previous menu.
```

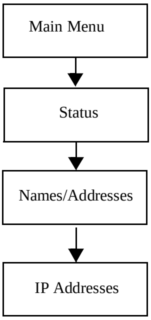
Figure 12-7 Verify Names & Addresses Commands Screen

3. Select **IP addresses**.

✓ The IP Addresses screen, shown in Figure 12-8, appears. This screen shows you the addresses as they are currently configured for each port and as they appear in the ARP table and in the Routing table.

```
                         *** IP Addresses ***


ARP Table:
IP Address        Port              MAC Address          Age


Routing Table:
Network Address Network Mask   Next Hop  Port    Metric    Age   VCN   Owner
133.1.0.0         255.255.0.0              7        0        0
100.0.0.0         255.0.0.0                0        0        0            LOC




________[DynaStar_3614]_________        Press <CTRL-F> to Flush the Tables.
Use XOFF <CTRL-S> and XON <CTRL-Q>                  Press <RET> for update.
                        to control scroll.   Press ESC to return to previous menu.
```

Figure 12-8 IP Addresses Screen



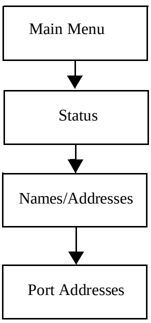
4. If you want to see the addresses for all ports (and not just those configured with an IP address), press **<ESC>** to return to the Verify Names & Addresses screen.

✓ The Verify Names & Addresses screen (Figure 12-7) appears.

5. Select **Port addresses (MAC, IPX, IP, X.121)**.

✓ The Port Addresses screen, similar to the one in Figure 12-9, appears.

NOTE: OSPF Addresses can be verified as described in the next section, *OSPF Routing*.




```
                         ***Port Addresses***

Port   Interface   MAC Address    IPX        IP          X.121
  0    ethernet    002061003614   00000000   100.1.1.1
  6    console
  7    X.25 line                  00001007   133.1.1.1   100
101    PPP                                   200.1.1.1
102    PPP                                   200.1.1.1
103    PPP                                   200.1.1.1
104    PPP                                   200.1.1.1

________[DynaStar_3614]_________          Press UP/DOWN to scroll.
                                  Press ESC to return to previous menu.
```

Figure 12-9 Port Addresses Screen

OSPF ROUTING

OSPF (Open Shortest Path First) is a routing scheme that operates over the IP protocol. It is a link state metric protocol that makes routing decisions based on link capacity, delay and throughput requirements, the number of data units presently in queue for transmission over a particular link, the number of hops required to reach a destination, and the ability to reach gateways and routers along the route. To take network dynamics into account, OSPF includes a weighting factor for each route. OSPF is considered a more robust protocol than RIP, which makes routing decisions based only on the number of hops to a destination.

To improve network efficiency, OSPF selectively limits route status messages and uses network partitioning and subnetting to control the amount of traffic and memory required to update router information. For example, one router can be designated to exchange routing tables with a local gateway, cutting down on the congestion that might occur if all routers

exchanged routing information with the gateway. As another example, Link State Advertisements are distributed only when there has been a change to network status. Further, if networks are designed correctly, sub-network status messages can be sent in a single Route Summarization message.

The remainder of this section explains how to configure the *DYNASTAR* for OSPF.

OSPF CONFIGURATION. OSPF configuration needs to be done in the order below:

- IP Address (required)
- OSPF Global Parameters (required)
- OSPF Area Parameters (required)
- OSPF Port Parameters (required)
- OSPF Range Parameters
- OSPF Virtual Link Parameters

All OSPF parameters are configured from the Router Commands menu. To access and configure these parameters, follow the procedure below:

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. Select **Router**.

✓ The Router Commands menu (Figure 12-2) is displayed.

3. Select **IP Port Information**.

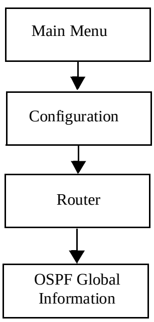
✓ The IP Port Information screen (Figure 12-3) is displayed.

4. Assign an IP address to each desired interface.

5. In the **Protocol** column, select **None** for the desired OSPF routed interfaces.

6. At the **Process IP Addresses** prompt, enter **Y <return>**.

✓ You return to the Router Commands menu.



7. Select **OSPF Global Information**.

✓ The OSPF Global Configuration screen (Figure 12-10) appears.

```
                         ***OSPF Global Configuration***
                                                  Last changed 4-23-02 13:55:20

     Router ID                    199.34.56.78     (4 bytes)
     Route Sharing                N                (Share routes with RIP)
     Automatic V-Link             N                <CR> to toggle

________[DynaStar_3614]_________                 Process selections (Y/N): Y
Use TAB & CURSOR keys to move among fields.Press ESC to abort command & exit
```

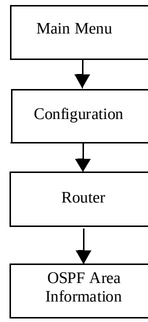
Figure 12-10 OSPF Global Configuration Screen

8. Configure the parameters as required. Parameters are explained in Table 12-2.

9. To save your configuration, enter **Y** in the **Process Selections** field and press **<return>**.

✓ Your selections are saved and you return to the Router Commands menu.

10. Select **OSPF Area Information**.



✓ The OSPF Area Information screen (Figure 12-11) appears.

```
                         ***OSPF Area Information***
                                          Last changed:  4-23-02  11:26:45
     Area ID       Authentication      Import AS        Stub Metric
     x.x.x.x           <CR>              <CR>             (1-255)
1:                     None               N                0
2:                     None               N                0
3:                     None               N                0
4:                     None               N                0
5:                     None               N                0
6:                     None               N                0
7:                     None               N                0
8:                     None               N                0
9:                     None               N                0
10:                    None               N                0



 ________[DynaStar_3614]_________          Process Table Selections (Y/N): Y
In Area ID field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.          Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

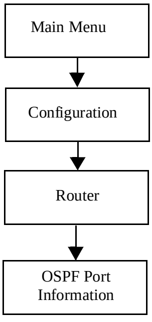
Figure 12-11 OSPF Area Information Screen

11. Configure the parameters as required. Parameters are explained in Table 12-3.

12. To save your configuration, enter **Y** in the **Process Selections** field and press **<return>**.

✓ Your selections are saved and you return to the Router Commands menu.

13. Select **OSPF Port Information.**



✓ The OSPF Port Information screen (Figure 12-12) appears.

```
                     ***OSPF Port Information***
                                        Last changed: 4-23-02  11:26:45
Port(s)   OSPF        Area ID     PRTY   Parameter   Value              Password
          <CR>        x.x.x.x    (0-255)   <CR>    (1-65535, 3600)      (0-8 ascii)
  0  BROADCAST    199.57.92.85    0      Transit       1
  3  NONE         0.0.0.0         0      Transit       1
  4  POINT-POINT  0.0.0.0         0      Transit       1
  5  POINT-POINT  0.0.0.0         0      Transit       1

 ________[DynaStar_3614]_________                Process OSPF ports (Y/N): Y
Lines with port ranges are multiport interfaces. Configure ports together or with cursor on
line, press <CTRL-O> to configure separately. *Fields are blank if ports are configured
separately. Press <CTRL-D> on metric value for default.
```

Figure 12-12 OSPF Port Information Screen

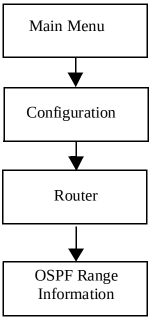
14. Configure the parameters as required. Parameters are explained in Table 12-4.

15. To save your configuration, enter **Y** in the **Process Selections** field and press **<return>**.

✓ Your selections are saved and you return to the Router Commands menu.

16. Select **OSPF Range Information.**

✓ The OSPF Range Information screen (Figure 12-13) appears.




```
***OSPF Range Information***
                                        Last changed:  4-23-02  11:26:45
     Range Net    Range Mask      Area ID          Status
     x.x.x.x      x.x.x.x         x.x.x.x          <CR>
1:   0.0.0.0      0.0.0.0         0.0.0.0          Advertise
2:   0.0.0.0      0.0.0.0         0.0.0.0          Advertise
3:   0.0.0.0      0.0.0.0         0.0.0.0          Advertise
4:   0.0.0.0      0.0.0.0         0.0.0.0          Advertise
5:   0.0.0.0      0.0.0.0         0.0.0.0          Advertise
6:   0.0.0.0      0.0.0.0         0.0.0.0          Advertise
7:   0.0.0.0      0.0.0.0         0.0.0.0          Advertise
8:   0.0.0.0      0.0.0.0         0.0.0.0          Advertise
9:   0.0.0.0      0.0.0.0         0.0.0.0          Advertise
10:  0.0.0.0      0.0.0.0         0.0.0.0          Advertise
11:  0.0.0.0      0.0.0.0         0.0.0.0          Advertise
12:  0.0.0.0      0.0.0.0         0.0.0.0          Advertise
13:  0.0.0.0      0.0.0.0         0.0.0.0          Advertise
14:  0.0.0.0      0.0.0.0         0.0.0.0          Advertise
15:  0.0.0.0      0.0.0.0         0.0.0.0          Advertise

 ________[DynaStar_3614]_________          Process Table Selections (Y/N): Y
In Range Net field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.            Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 12-13 OSPF Range Information Screen

17. Configure the parameters as required. Parameters are explained in Table 12-5.

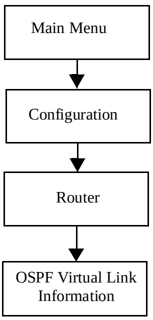
18. To save your configuration, enter **Y** in the **Process Selections** field and press **<return>**.

✓ Your selections are saved and you return to the Router Commands menu.

19. Select **OSPF Virtual Link Information.**

12

The IP/IPX Router Application



✓ The OSPF Virtual Link Information screen (Figure 12-14) appears.

```
                    ***OSPF Virtual Link Information***
                                        Last changed:  1/26/99  11:26:45
     Transit ID  Router ID    Parameter      Value        Autype     Password
      x.x.x.x     x.x.x.x       <CR>     (1-65535, 3600)   <CR>     (0-8 ascii)
1:   199.97.34.56198.12.34.56 Transit        1             None        60
2:   0.0.0.0      0.0.0.0     Transit        0             None
3:   0.0.0.0      0.0.0.0     Transit        0             None
4:   0.0.0.0      0.0.0.0     Transit        0             None
5:   0.0.0.0      0.0.0.0     Transit        0             None
6:   0.0.0.0      0.0.0.0     Transit        0             None
7:   0.0.0.0      0.0.0.0     Transit        0             None
8:   0.0.0.0      0.0.0.0     Transit        0             None
9:   0.0.0.0      0.0.0.0     Transit        0             None
10:  0.0.0.0      0.0.0.0     Transit        0             None

 ________[DynaStar_3614]_________                 Process selections (Y/N): Y
In Transit ID field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.          Use <CTRL-D> to delete entry.
```

Figure 12-14 OSPF Virtual Link Information Screen

20. Configure the parameters as required. Parameters are explained in Table 12-6.

21. To save your configuration, enter **Y** in the **Process Selections** field and press **<return>**.

✓ Your selections are saved and you return to the Router Commands menu. Your OSPF configuration is now complete.

Table 12-2 OSPF Global Information Parameters

Parameter	Description	Values
Router ID	OSPF router ID for this *DynaStar* distinguishing it from all others in the Autonomous System. This is typically the IP address of the *DynaStar*'s Ethernet port, if in use, or any other IP address assigned to a physical interface in step 4 of this procedure.	0.0.0.0 - 255.255.255.255 (4 bytes) Default = 0.0.0.0
Route Sharing	If set to Yes, routing information is exchanged with the *DynaStar*'s RIP router.	Y, N Default = N
Automatic V-Link	If set toYes, enables automatic generation of virtual links. (Virtual links are required to restore backbone connectivity when the Autonomous System is divided into non-contiguous areas.) NOTE: To be able to configure virtual links, the *DynaStar* must be an area border router. If this parameter is set to No, all required virtual links must be configured manually.	Y, N Default = N

Table 12-3 OSPF Area Parameters

Parameter	Description	Values
AreaID	IP-like address unique to this particular area. The backbone area is typically set for 0.0.0.0	0.0.0.0 - 255.255.255.255 (4 bytes) Default = 0.0.0.0
Authentication	If set to None, no password is required. If set to Simple, a password must be defined on the OSPF port configuration menu, and all packets sent on the network must carry this value in the OSPF header.	None (Default) Simple
Import AS	If set to Yes, external advertisements are flooded through this area. The parameter must be set to Yes for the backbone and areas connected to the backbone by a virtual link. Set to No for a Stub area. Routing tables will maintain information for the entire area, regardless of the value of this parameter.	Y, N Default = N
Stub Metric	Applies to stub areas only. Determines the routing “cost” of the default line. Stub areas are areas into which OSPF does not flood AS (autonomous system) external advertisements. You might want to configure stub areas if much of the topological database consists of AS external advertisements, and you want to minimize the size of the topological databases on an area’s routers.	1-255 Default = 0

Table 12-4 OSPF Port Parameters

Parameter	Description	Value
OSPF	Indicate type of OSPF routing enabled on this interface. Set to Broadcast for LAN ports and Point-Point for WAN ports.	Broadcast Point-Point None
AreaID	Identifier of OSPF area to which the port (interface) belongs, as defined in the Area parameters. 0.0.0.0 is the backbone area. It is suggested that you use a subnet address, but this is not required.	0.0.0.0 - 255.255.255.255 (4 bytes) Default = 0.0.0.0
Priority	Valid only for LAN ports. Priority used to determine whether this router will become the network's designated router. 0=this router is ineligible to be the designated router. 255 is the highest priority. 255 means that this router is responsible for sending network link advertisements, which describe all the routers attached to the network. These advertisements are flooded throughout a single area. At least one router on each logical IP network or subnet must be eligible to be the designated router.	0-255 Default = 0

The following parameters are toggle fields under the "Parameter" column:

Table 12-4 OSPF Port Parameters (cont.)

Parameter	Description	Value
Transit (Transit Delay)	How often Link State Advertisement packets are sent over this interface. This interval determines the maximum packet transmission rate on an interface, which affects network stability. Because packets are built at the instant of transmission, only the latest information is sent even if the transmission is delayed. When configuring the Transit Delay, take into account the transmission and propagation delays that occur on this interface. For example, increase the value for low-speed serial connections. The default value, one second, is appropriate for a LAN connection.	1-3600 seconds Default = 1
Retran (Retransmit Interval)	The time between retransmissions of link state advertisements when an acknowledgment is not received. This parameter is used for adjacencies that belong to this interface and for retransmissions of OSPF Database Description and Link State Request packets. Set this parameter to a value that is higher than the expected round-trip delay between any two routers on the network attached to this port. Otherwise, needless retransmissions will occur. The default value, 5 seconds, is appropriate for a LAN connection. Low-speed links require a higher value.	1-3600 seconds Default = 5

Table 12-4 OSPF Port Parameters (cont.)

Parameter	Description	Value
Hello (Hello Interval)	The length of time, in seconds, between Hello packets that the *DYNASTAR* sends on this interface. Must be the same value for all routers that connect to the interface's network. If you set the Hello Interval to a short length of time, changes to the OSPF topological database will be detected more quickly, but more OSPF routing protocol traffic will be generated. The default value, 10 seconds, is suggested for a LAN connection. A PVC may require a Hello Interval of 30 seconds.	1-3600 seconds Default = 10
Dead (Dead Interval)	The length of time, in seconds, before neighboring routers declare a router down when they stop receiving its Hello Packets. The value of the Dead Interval parameter is advertised in Hello Packets sent out from this interface and must be the same on all other routers connected to this interface. Set the Dead Interval to a multiple of the Hello Interval.	1-3600 seconds Default = 40
Metric	Cost, or weight, of sending a packet on this interface. NOTE: The same basis for determining the metric (for example, speed, throughput, or line cost) should be used throughout the network.	1-65535 Default = 1
Password	Eight character authentication: Must be the same for all routers in an area.	0 to 8 ASCII characters Default = No value

Table 12-5 OSPF Range Parameters

Parameter	Description	Values
Range Net	Together with the Range Mask, identifies a group of subnets in this address range. Routers may belong to multiple areas, depending on their attached networks. When configuring the Range Net values for all address ranges, keep all subnetted networks in the same area. NOTE: Ranges are required only for those areas that connect to the backbone via an area border router.	0.0.0.0 - 255.255.255.255 (4 bytes) Default = 0.0.0.0
Range Mask	Together with Range Net, identifies a group of subnets in this address range.	0.0.0.0 - 255.255.255.255 (4 bytes) Default = 0.0.0.0
AreaID	Unique address as defined for this range.	0.0.0.0 - 255.255.255.255 (4 bytes) Default = 0.0.0.0
Status	If set to Advertise, a single route is advertised for this address range on a summary link advertisement that is external to the area. If set to Hide, no route is advertised for this address range. This setting allows you to hide certain networks from other areas.	Advertise (Default) Hide

Table 12-6 OSPF Virtual Link Parameters

Parameter	Description	Values
Transit ID	Unique area identifier for the area that the virtual link passes through.	0.0.0.0 - 255.255.255.255 (4 bytes) Default = 0.0.0.0
Router ID	Router identifier for the other endpoint of the virtual link (neighbor ID)	0.0.0.0 - 255.255.255.255 (4 bytes) Default = 0.0.0.0
The following parameters are toggle fields under the “Parameter” column:		
Transit (Transit Delay)	How often Link State Advertisement packets are sent over this interface. This interval determines the maximum packet transmission rate on an interface, which affects network stability. Because packets are built at the instant of transmission, only the latest information is sent even if the transmission is delayed. When configuring the Transit Delay, take into account the transmission and propagation delays that occur on this interface. For example, increase the value for low-speed serial connections. The default value, one second, is appropriate for a LAN connection.	1-3600 seconds Default = 1

Table 12-6 OSPF Virtual Link Parameters (cont.)

Parameter	Description	Values
Retran (Retransmit Interval)	The time between retransmissions of link state advertisements when an acknowledgment is not received. This parameter is used for adjacencies that belong to this interface and for retransmissions of OSPF Database Description and Link State Request packets. Set this parameter to a value that is higher than the expected round-trip delay between any two routers on the network attached to this port. Otherwise, needless retransmissions will occur. The default value, 5 seconds, is appropriate for a LAN connection. Low-speed links require a higher value.	1-3600 seconds Default = 5
Hello (Hello Interval)	The length of time, in seconds, between Hello packets that the *DynaStar* sends on this interface. Must be the same value for all routers that connect to the interface's network. If you set the Hello Interval to a short length of time, changes to the OSPF topological database will be detected more quickly, but more OSPF routing protocol traffic will be generated. The default value, 10 seconds, is suggested for a LAN connection. A PVC may require a Hello Interval of 30 seconds.	1-3600 seconds Default = 10

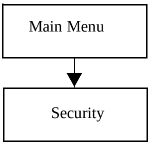
Table 12-6 OSPF Virtual Link Parameters (cont.)

Parameter	Description	Values
Dead (Dead Interval)	The length of time, in seconds, before neighboring routers declare a router down when they stop receiving its Hello Packets. The value of the Dead Interval parameter is advertised in Hello Packets sent out from this interface and must be the same on all other routers connected to this interface. Set the Dead Interval to a multiple of the Hello Interval.	1-3600 seconds Default =40
Autype	Authentication Type. If set to None, no password is required. If set to Simple, a password must be defined on the OSPF port configuration menu, and all packets sent on the network must carry this value in the OSPF header.	None (Default) Simple
Password	Eight character authentication. Must be the same for both routers on the virtual link.	0 to 8 ASCII characters Default = No value

IP FILTERING

IP filtering allows call blocking or forwarding based on specific IP addresses or address masks, as well as on FTP, Telnet, Ping, and World-Wide Web applications. Subnet mask support is also available. You can use the IP Filter table to designate a default IP filtering action and create up to 60 specific filtering actions.

The IP Filter searches from the top of the table and performs a filtering action based on the first match that it finds for an address. If no match is found for either the source or destination address, the call is blocked or forwarded based on the selection in the **Default filter action** field. This field is initially configured to forward all traffic.



To configure the IP filters:

1. From the Main menu, select **Security**.

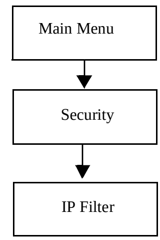
✓ The Security Commands menu, shown in Figure 12-15, appears.

```
                    ***Security Commands***

      1 - Password Change          Change Operator Password
      2 - Access Security          Change Operator Access
      3 - IPX-In Security          IPX-In ID strings
      4 - IPX-Out Security         IPX-Out service restrictions
      5 - IP Filter                IP Address Filter
      6 - TL1 Security             Add/Change TL1 Username/Password
      7 - Network Security         Add/Change Network Passwords
      8 - Destinations             Add/change Permitted Destinations
      9 - Security Options         Validation options and methods
     10 - SecurID                  Access Authorization
     11 - Port Selection           Which ports have security enforced

________[DynaStar_3614]________
Terminate input with <RET>.          Press ESC to return to previous menu.
```

Figure 12-15 Security Commands Menu

2. Select **IP Filter**.

✓ The IP Filter table, as shown in Figure 12-16, is displayed.




```
                              ***IP Filter Table***
                                        Last changed:  4-23-02  11:26:45
  Class     Source IP   Mask     Destination IP   Mask    FTP  TEL  PNG  WWW  OTH
 (Toggle)  (Address)  (# Bits)    (Address)     (# Bits)            (Toggle)
1:
2:
3:
4:
5:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:
Default Filter Action:   FTP   TEL   PNG   WWW  OTH
                         FWD  FWD  FWD   FWD   FWD

 ________[DynaStar_3614]_________               Process IP Filter table (Y/N): Y
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 12-16 IP Filter Table

3. With your cursor in the **Class** column, press **<return>** to select the desired option:

   - **B** (Both) filters on both the source and destination addresses configured.
   - **S** (Source) filters on only the specific IP source address configured.
   - **D** (Destination) filters on only the specific IP destination address configured.
   - **NB** (Netboth) filters both the source and destination addresses based on the masks entered on the same line.
   - **NS** (Netsource) filters the source network address based on the mask entered on the same line.
   - **ND** (Netdest) filters the destination network address based on the mask entered on the same line.

4. Tab to the **Source IP**, **Destination IP**, and/or **Mask** fields as appropriate and enter a complete address or mask as required for the type of filtering you are configuring.

5. In the specific applications columns, toggle to select Block (**BLK**) or Forward (**FWD**), as appropriate.

6. Once you have filled in all specific actions, move to the **Default filter action** field at the bottom of the screen and select **FWD** or **BLK** as the action to be performed on addresses that either do not appear in the table or cannot be derived from masks that appear in the table.

   NOTE: If you are filtering specific IP applications (such as FTP or Telnet), set the **OTH** field at the bottom of the screen to **FWD**.

7. When all of your entries are complete, enter **Y** in the **Process IP filter table** field and press **<return>**.

✓ You return to the Security Commands screen. When you redisplay the IP Filter table, the actions will have been resorted by class and address as described in the section *Table Sorting.*

   NOTE: In the sorted table, an address or mask of *.*.*.* indicates “Don’t care” and is not used for filtering.

TABLE SORTING. Actions in the IP filter table are sorted as follows:

1. Entries with specific addresses appear before entries with masks.

2. Addresses and masks are sorted from low to high values.

3. Actions are sorted (in order of decreasing priority) by class as follows:

   - BOTH (source and destination address)
   - SOURCE (source address only)
   - DESTINATION (destination address only)

- NETBOTH (both source and destination network masks)
- NETSOURCE (source network mask only)
- NETDESTINATION (destination network mask only)

APPLICATION ROUTING

With application routing, you can define two WAN links to a single IP destination and then specify which calls will use which link, based on the call's application process. The IP routing function sees the two physical links as a single logical link.

Figure 12-17 shows an example of how you might use application routing. In this scenario, there are two WAN links from the *DYNASTAR* to the IP network. These links are an X.25 connection over the ISDN D-channel and PPP over the ISDN B-channel. However, any number or type of connections (X.25, frame relay, dedicated PPP, or dial PPP) can be used.

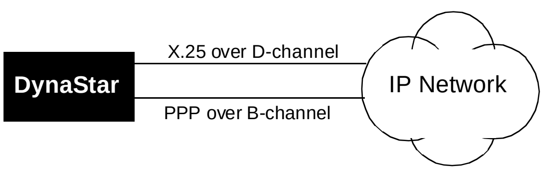


Figure 12-17 Two Routes to IP Network

In order to use application routing, you must first configure the two (or more) connections to the IP network. These connections are configured in the same way that you configure any connection, as explained in the previous section. It does not matter which connection is defined first.

Once the connections are defined, you must then complete the final step of defining the application routes.

ROUTING ENTRIES. Before you can define the application routes, you must understand the constituent parts of a route. A route is defined by a port number and a *qualifier*.

What the qualifier consists of depends on the type of route, as shown in Table 12-7.

Table 12-7 Routing Types

Type of Route		Qualifier
X.25	= Port # +	X.121 address
Frame Relay	= Port # +	DLCI
PPP	= Port # +	No qualifier (if direct connect) Name (if dial directory entry)

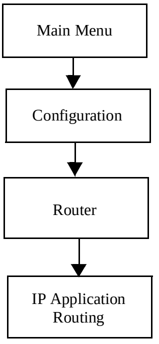
To configure an application route:

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) appears.

2. Select **Router**.
3. The Router Commands menu (Figure 12-2) appears.
4. Select **IP application routing**.

✓ The IP Application Routes screen, as shown in Figure 12-18, appears.




```
                         ***IP Application Routes***
                                              Last changed: 4-23-02  11:26:45

       Default           Redirection
    Port   Qualifier    Port    Qualifier         TCP        UDP        ICMP
0001   5       1        PD       3001             TELNET     TFTP
0002
0003
0004
0005
0006
0007
0008
0009
0010
0011
0012
0013
0014
0015
Note: 'PD' specifies a dial PPP port. To DELETE use <CTRL-D>.


________[DynaStar_3614]_________        Process Application Routes (Y/N): Y
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 12-18 IP Application Routes Screen

5. In the **Default Port** field, toggle through the available ports until the port number you want is displayed. This port will handle all traffic other than that explicitly defined to use a redirection port. If you have not yet configured the port, you can enter the number manually. (**PD** appears for a dial PPP port.)

6. In the **Default Qualifier** field, enter the correct qualifier. Qualifiers for the various types of routing entries are given in Table 12-7. (There is no qualifier for a dedicated PPP connection.)

   NOTE: You are not required to indicate a qualifier for the default port if you do not want to restrict the routing type.

7. In the **Redirection Port** field, toggle through the available ports until the port you want is displayed. This port will handle the traffic (application process) explicitly defined in this entry. If you have not yet configured the port, you can enter the number manually. (**PD** appears for a dial PPP port.)

8. In the **Redirection Qualifier** field, enter the correct qualifier. You are required to enter a qualifier unless the connection type is dedicated PPP.

9. In the **TCP** field, indicate the application process, if any, that will use this protocol and the defined redirection port.

NOTE: You can toggle through common application processes (for example, **FTP**, **Telnet**, **WWW**, or ***** [all] for TCP). You can also manually enter any other application process. See the section *Application Processes* that follows.

NOTE: If you want more than one TCP application to use the redirection port, you must make additional entries in the table with the same default and redirection ports but with different TCP application processes. The same is true if you are directing multiple UDP and/or ICMP application processes to the redirection port.

10. In the **UDP** field, indicate the application process that will use this protocol and the defined redirection port. You can toggle through common UDP application processes (**TFTP**, **SNMP**, ***** [all]).

11. In the **ICMP** field, indicate the application process that will use this protocol and the defined redirection port. You can toggle through common ICMP application processes (**Ping** and ***** [all]).

12. When you have completed your configuration, enter **Y** in the **Process Application Routes** field and press **<return>**.

APPLICATION PROCESSES. The application processes using the various Internet protocols identify themselves with a port number, also called a "well-known port number." This number is used between the sending and receiving entities to identify the application process that is to receive the incoming traffic. This also provides a multiplexing capability by

allowing multiple user programs to communicate concurrently with one application program, such as TCP or UDP.

Port numbers for frequently used application processes, such as Telnet and TFTP, are preassigned. These port numbers use the range 0 to 255. If you wish to assign a port number to your own application process, you should use a number greater than 255. A list of some of the commonly assigned port numbers is given in Table 12-8.

Table 12-8 Internet Port Numbers

Port Number	Process Name	Description
5	RJE	Remote Job Entry
7	ECHO	Echo
11	USERS	Active users
13	DAYTIME	Daytime
20	FTP-DATA	File Transfer (Data)
21	FTP	File Transfer (Control)
23	TELNET	Telnet
25	SMTP	Simple Mail Transfer
37	TIME	Time
42	NAMESERV	Host Name Server
43	NICKNAME	Who Is
53	DOMAIN	Domain Name Server
67	BOOTPS	Bootstrap Protocol Server
68	BOOTPC	Bootstrap Protocol Client
69	TFTP	Trivial File Transfer
79	FINGER	Finger
101	HOSTNAME	NIC Host Name Server
102	ISO-TSAP	ISO-TSAP
103	X400	X.400

Table 12-8 Internet Port Numbers (cont.)

Port Number	Process Name	Description
104	X400SND	X.400 SND
105	CSNET-NS	CSNET Mailbox Name Server
109	POP2	Post Office Protocol 2
111	RPC	SUN RPC Portmap
137	NETBIOS-NS	NETBIOS Name Service
138	NETBIOS-DG	NETBIOS Datagram Service
139	NETBIOS-SS	NETBIOS Session Service

TCP/IP MULTICAST APPLICATION

The *DYNASTAR* supports a broadcast feature. You can define a maximum of 16 TCP sources, each of which can connect to a maximum of 16 TCP destinations. Traffic received on the source IP address and socket is sent to each of the destinations; any traffic received on the destinations is sent only to the source.

When a user connects to the source IP address and socket, TCP connections are automatically launched to the destinations. If a destination is cleared, the *DYNASTAR* attempts to reestablish the connection every 10 seconds. If the source is cleared, all destinations are cleared.

To configure the multicast application:

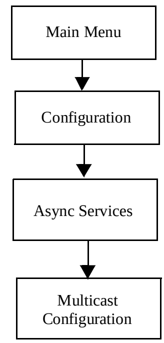
1. Configure the source by configuring a Multicast async service type. See *Configuring the Async Services Menu* in Chapter 13, *Telnet and Async Services*. Only the IP address and socket need to be defined.
2. To configure the destinations, select **Configuration** from the Main menu.

✓ The Configuration Commands menu (Figure 3-11) appears.

3. From the Configuration Commands menu, select **Async Services**.

4. From the Access Server Comands menu that appears, select **Multicast Configuration**.

✓ The Multicast Destinations screen (Figure 12-19) appears.




```
                        *** Multicast Destinations ***
                                        Last changed: 4-23-02  11:26:45

  IP Address      Socket          Source Socket           Source Name

1.





 ________[DynaStar_3614]_________                Process selections (Y/N): Y
Use <CTRL-D> to delete entry                 <RET> to toggle or type value
Use TAB & CURSOR keys to move among fields. Press ESC to return to previous menu.
```

Figure 12-19 Multicast Destinations Screen

5. Enter the IP address and socket of the destination in the **IP Address** and **Socket** columns.

6. In the **Source Socket** column, toggle to obtain the source socket for this destination.

7. In the **Source Name** column, toggle to obtain the source name for this destination.

NOTE: Destinations can be terminated on the same *DynaStar* as the source. They can be converted to X.25 via X25-OUT async services (see Chapter 13) or they can be routed to another device.

8. When you have completed your configuration, enter **Y** in the **Process selections** field and press **<return>**.

BOOTP RELAY AGENT

The *DYNASTAR* can act as a BOOTP relay agent to transfer BOOTP messages between clients and servers. BOOTP (Bootstrap Protocol or Boot Protocol) is an alternative to RARP. Its name comes from the fact that it is designed to be contained within a diskless workstation's bootstrap ROM. It goes beyond RARP by getting the path and filename of the bootstrap file as well as its default router, its own IP address, and the BOOTP server's IP Address.

One of the reasons that many systems are using BOOTP instead of RARP is the capability of reaching the BOOTP server beyond a router. In fact, the BOOTP server can be several hops away from the BOOTP client system.

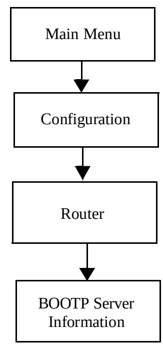
Whereas RARP is carried by the Network Access Layer, BOOTP, as a TCP/IP application, sends its messages in UDP headers enclosed in IP datagrams. In many cases, BOOTP clients and their associated BOOTP server(s) do not reside on the same IP network or subnet. In such a case, a *DYNASTAR* can act as a relay agent to transfer BOOTP messages between clients and servers.

To configure the *DYNASTAR* to act as a BOOTP relay agent follow the procedure below:

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) appears.

2. Select **Router**.
3. The Router Commands menu (Figure 12-2) appears.
4. Select **BOOTP Server Information**.



✓ The BOOTP Server Information screen, as shown in Figure 12-20, appears.

```
                    *** BOOTP Server Information ***
                                      Last changed: 4-23-02  11:26:45

     BOOTP Server        LAN
     IP Address          Interface
     x.x.x.x.x
1:
2:
3:
4:
5:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:

 ________[DynaStar_3614]_________          Process BOOTP Server Info (Y/N): Y
In Server address field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value            Use <CTRL-D> to delete entry
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 12-20 BOOTP Server Information Screen

5. In the **BootP Server IP Address** field, enter the address of the BOOTP server to which the *DynaStar* will forward the BOOTP requests it receives on its LAN interfaces. You can configure a maximum of 15 BOOTP server addresses.

NOTE: The requests may or may not actually be forwarded, depending on the value in the **LAN Interface** field (see step 6).

6. In the **LAN Interface** field, enter one of the following values:

- **ALL**: Use the server defined in the **BootP Server Address** field for BOOTP requests on all the LAN interfaces.
- **NONE**: Do not forward any requests to the server defined in the **BootP Server Address** field (temporarily disable the service for this address).

- **Port Number**: Use the server defined in the **BootP Server Address** field only for the requests received on this LAN port.

7. When you have completed your configuration, enter **Y** at the **Process BOOTP Server Info** prompt and press **<return>**.

■ THE IPX ROUTER

The IPX router lets LAN workstations access a distant server (such as file servers, FAX servers, or communications servers) on any interconnected NetWare LAN.

CONFIGURING THE *DYNASTAR* FOR IPX ROUTING

1. Configure the correct protocol for the port you will be using.
   - For an X.25 port, see Chapter 6.
   - For a frame relay port, see Chapter 8.
   - For a PPP port, see Chapter 10.
2. Make sure that IPX routing is enabled for these ports.
3. If you enabled IPX routing for a dial connection, you must establish SAP static routes. Continue with steps 4 through 12.

   NOTE: You can configure a maximum of 60 SAP static routes.
4. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) appears.

5. Select **Router**.

✓ The Router Commands menu, as shown in Figure 12-2, appears.

6. Select **IPX SAP static routes**.

✓ The IPX SAP Static Routes menu, as shown in Figure 12-21, is displayed.

7. In the **Server Name** column, enter the name of the remote destination server and press **<return>**.

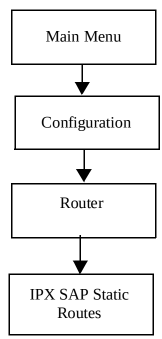
✓ Default values are filled in for the remaining columns and the cursor moves to the **Server Type** column.

8. The default value displayed in the **Server Type** column is for a file server (0004). Change this number only if the remote server is not a file server.

> **NOTE:** If you press **?<return>** while the cursor is in the **Server Type** column, a list of server types is displayed (see Figure 12-22).

```
                         ***IPX SAP Static Routes***
                                        Last changed:  4-23-02  11:26:45

                     Server Type    Network     Node            Socket
  Server Name        ?<RET>         Number      Number          Number    Hops
  (1-32 characters)  for list       (8 hex)     (12 hex)        (4 hex)   (1-15)
1: PLUTO              0004        000012AC   00AC1FFA2CEF      0451        1
2:
3:
4:
5:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:
 ________[DynaStar_3614]_________          Process SAP static routes (Y/N): Y
In server name field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.          Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 12-21 IPX SAP Static Routes Menu



Server Types up to 0x8000 are reserved by Novell for well-known server types. Other types may be defined and used by third-party applications as needed. If a general-purpose type is needed, call 1-900-SAY-HELP for assignment.

List of Common Servers:

0000 - Unknown	0007 - Print Server
0001 - User	0008 - Archive Queue
0002 - User Group	0009 - Archive Server
0003 - Print Queue	000A - Job Queue
0004 - File Server	000B - Administration
0005 - Job Server	0023 - Async Server
0006 - Gateway	0024 - Remote Bridge Server

Press ESC to exit from Help.

Figure 12-22 Server List

9. In the **Network Number** column, enter the number of the remote Novell LAN where the server resides. This is the call's final destination.
10. Enter the remote node number and socket number in the appropriate columns if these must be specified to reach the destination.
11. In the **Hops** column, enter the number of hops to the remote network using this static route.
12. When your selections are complete, enter **Y** in the **Process SAP static routes** field and press **<return>**.

✓ The static routes become available immediately.

If the SAP entry you just created is not the default route, that is, if you set the selection **Use as Default IPX route** to **N** in the PPP Dial Directory screen, you must also configure a RIP static route. You can configure a maximum of 120 RIP static routes. (See Chapter 10, *The PPP Application*, for more information on setting the default IPX route.)

To establish an IPX RIP static route:

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. Select **Router**.

✓ The Router Commands screen, shown in Figure 12-2, is displayed.

3. Select **IPX RIP static routes**.

✓ A menu similar to the one in Figure 12-23 is displayed.

4. In the **Remote Destination Network Number** column, enter the network number for the remote destination server.

   NOTE: This number must match your entry for **Network Number** in the IPX SAP Static Route table.

✓ Default values appear in the other columns and the cursor moves to the **Next Network** column.

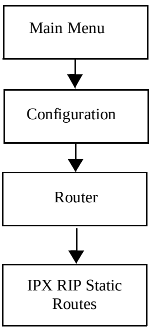
5. In the **Next Network** column, enter the number of the next network on the path to the destination. (This is the logical IPX network formed by the two PPP ports used in the call. This entry must match the entry in the **Novell Network** field in the PPP dial directory entry for this destination.)

6. In the **# of Hops** column, indicate the number of hops to the next network.

7. In the **Delay Ticks** column, indicate the estimated amount of time for transferring an IPX frame across the line (18 ticks = 1 second).

8. When your selections are complete, enter **Y** in the **Process RIP static routes** field and press **<return>**.

✓ The static routes become available immediately.




```
                         ***IPX RIP Static Routes***
                                        Last changed:  4-23-02  11:26:45

    Remote Destination    Next Network       # of Hops to      Delay
    Network Number        in the Route       Next Network      Ticks
    (8 HEX Digits)        (8 HEX Digits)     (1-15)            (1-360)
1:  00000001              00000002             1                 60
2:
3:
4:
5:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:
 ________[DynaStar_3614]_________          Process RIP static routes (Y/N): Y
In remote network field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.          Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 12-23 IPX RIP Static Routes Menu

CHECKING YOUR IPX ADDRESSES. Once you have configured your IPX addresses, you can verify your entries for all IPX ports in the IPX Addresses menu.

1. From the Main menu, select **Status**.

✓ The Status Commands menu (Figure 12-6) appears.

2. Select **Names/Addresses**.

✓ The Verify Names & Addresses Commands screen (Figure 12-7) appears.

3. Select **IPX addresses**.

✓ The IPX Addresses screen, shown in Figure 12-24, appears. This screen shows you the addresses as they are currently configured for each IPX port.

*** IPX Addressess ***

Network	Port	Hops	Ticks	Age
00354201	0	0	1	0
00422e00	1	0	1	0
00000002	0	1	2	7
00000003	0	1	2	7
00356a06	0	1	181	5

Type	Server Name	Network	Node	Socket	Hop	Port	Age
0004	COPERNICUS	00000002	000000000001	0451	1	0	20
0047	TSIOLKOVSKY	00000002	000000000001	8060	2	0	20
04D3	EINSTEIN	00422E00	0020610035FF	82DF	1	0	20
0026	EINSTEIN	00422E00	0020610035FF	4003	1	0	20

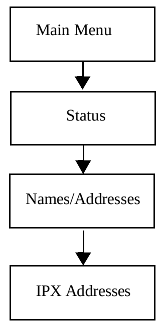
________[DynaStar_3614]_________

Use XOFF <CTRL-S> and XON <CTRL-Q> to control scroll.

Press <RET> for update.

Press ESC to return to previous menu.

Figure 12-24 IPX Addresses Screen



4. If you want to see the addresses for all ports (and not just those configured with an IP address), press **<ESC>** to return to the Verify Names & Addresses screen.

✓ The Verify Names & Addresses screen (Figure 12-7) appears.

5. Select **Port addresses (MAC, IPX, IP, X.121)**.

✓ The Port Addresses screen, similar to the one in Figure 12-9, appears.

IPX RIP/SAP SPOOFING

On an Ethernet network, RIP/SAP spoofing provides the ability to prevent RIP/SAP messages from propagating across WAN ports. This is useful on ISDN dial connections, since it would be impractical and costly to send out these messages every 30 to 60 seconds. When spoofing is used, RIPs and SAPs are transferred across the WAN only when updates are required or on a regular (timed) basis.

This means that a local *DYNASTAR* spoofs RIPs and SAPs from the remote file server and transmits them to its local Ethernet users so that the remote server appears to local users to be available through a router connection. When one of these users requests a connection, the *DYNASTAR* places a call to the remote server. If there is no activity of any type on the line for the amount of time configured for the **Dial IPX traffic idle timer**, the call is disconnected. (See Chapter 10, *The PPP Application*, for more information on the idle timers.)

To set RIP/SAP parameters:

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) appears.

2. Select **Router**.

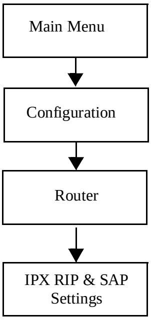
✓ The Router Commands menu, shown in Figure 12-2, appears.

3. Select **IPX RIP & SAP settings**.

✓ A menu similar to the one in Figure 12-25 is displayed.

4. In the field **Send SAP broadcast onWAN for** , select either **All Servers** or **File Servers only**. This controls the services advertised over the WAN connection to the remote network.

5. In the field **Send RIP & SAP broadcasts on changes**, select **Y** if you want updates to be propagated across the WAN if they occur when a connection is up. Select **N** if updates are to be saved and sent as part of a scheduled RIP and SAP transmission.



6. After **Send RIP & SAP broadcasts every**, enter **0** to disable RIP and SAP transmissions across the WAN. Or enter a value from 1 to 120 to indicate in minutes how often RIPs and SAPs are to be sent across the WAN.

```
                         ***RIP/SAP Settings***
                                    Last changed:  4-23-02  11:26:45
              ------------ Press <RET> to toggle values ------------

 Send SAP broadcast on WAN for:                 All Servers

 Send RIP & SAP broadcasts on changes:          N

                    ------------ Type in values ------------

 Send RIP & SAP broadcasts every:               1            (0-disable, 1-120 min)

 Keep alive after disconnect for:               30           (0-disable, 1-255 min)




________[DynaStar_3614]_________                Process selections (Y/N): Y
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 12-25 RIP/SAP Settings

7. Determine how spoofing will be used in the field **Keep alive after disconnect for**. Enter **0** if no keep alives are to be sent when theWAN call is disconnected. Or enter a value from 1 to 255 to indicate how many minutes the *DynaStar* will continue to send spoofed Keep Alive messages to its local Ethernet users.

8. When your selections are complete, enter **Y** in the **Process Selections** field and press **<return>**.

Accessing the IPX Router

1. From the workstation, log on to the nearest file server.
2. Issue the NetWare SLIST command to see which file servers are available and which networks they are located on. The *DynaStar* IPX Server table supports up to 200 servers in the network.
3. Execute the ATTACH or LOGIN command to access a file server on another NetWare LAN. You must be logged on to a file server before using the ATTACH utility.

Please refer to the appropriate NetWare documentation for information about these commands. Procedures to access other types of servers (such as a FAX server) are embedded in the user application. The connection to a distant NetWare LAN is transparent to the user except for any delay introduced by the connection. Delay is a function of the line speed, the number of simultaneous users that are actively sending information on the line, and the volume of traffic being transmitted. IPX traffic flow is regulated by Novell RIP. The *DynaStar* automatically sets NetWare addresses and uses other configuration parameters to establish and maintain a link between each pair of IPX routers.

■ IPX-In

IPX-In allows an asynchronous device (such as a PAD or modem) to connect through the *DYNASTAR* to a Novell LAN running Netware. The connection can be made through dial-up lines or over an X.25 network, as shown in Figure 12-26 and Figure 12-27.

For direct dial-up access, the Sync/Async port or any of the asynchronous ports on the optional OCTAL+, QUAD, or 8 or 16-port cards can be configured for IPX-In.

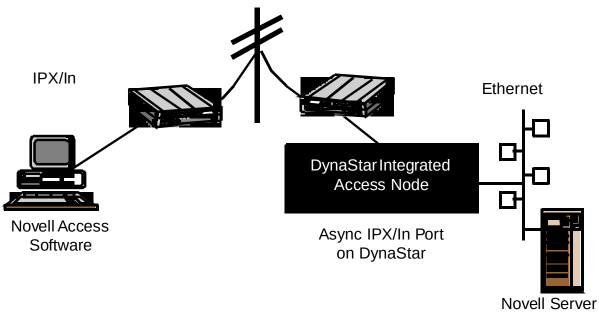


Figure 12-26 IPX-In over Dial-up Lines

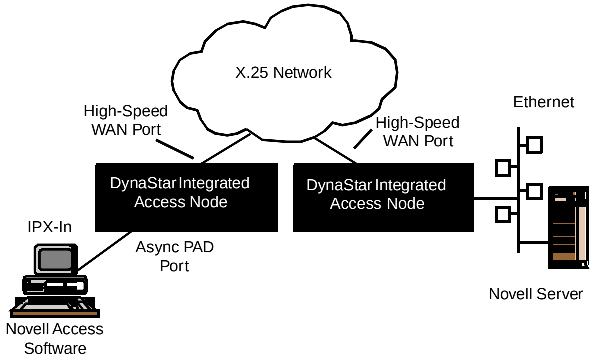


Figure 12-27 IPX-In over an X.25 Network

CONFIGURATION OF THE *DYNASTAR*

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) appears.

2. Select **Port**.

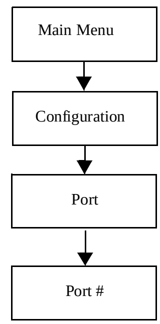
✓ A list of available ports appears.

3. Select the port that you want to configure as IPX-In and enter that port's number in the **Enter port number** field.

✓ The Port Configuration screen appears.

4. Set the **Port type** to **IPX-In** or **IPX-In/Out**.

✓ The screen displays the parameters that need to be configured for IPX-In, as shown in Figure 12-28.




```
                    ***Asynchronous Port Configuration***
                                          Last changed: 6-6-02  11:26:45
 Port: 7  IS-35

 |---  Press <RET> to toggle values  --||--- Type in values.  Max chars shown in ()  ---|
 Port type:    IPX-In              Port name:       Sync/Async                       (14)


Connection mode:     DIAL             Modem command:       &Q0S37=9              (25)
Modem speed:         9600 baud        Life class timer:    30     (0-disable, 1-60 min)

Parity:              8-NONE
Flow control:        NONE             IPX network address:  00000000           (8 HEX)




 ________[DynaStar_3614]_________                  Process selections (Y/N): Y
  UseTAB & CURSOR keys to move among fields.   Press ESC to abort command & exit.
```

Figure 12-28 IPX-In Port Configuration Screen

5. Select the appropriate connection mode.

   - **Dial** makes the port appear as a DTE. This selection is used for dial-out connections.
   - **DCE** makes the port appear as a DCE. This selection is used for connection to a terminal.
   - **DTE** makes the port appear as a DTE. This selection is used for connection to a modem.

6. Set the **Modem speed** and **Flow control** to be consistent with settings in the PC Arconfig file (see the next section, *Configuration of the PC*). **Parity** is set to **8-NONE** and cannot be changed.

7. If you selected **Dial** as the **Connection mode**, enter an appropriate **Modem command** and **Life class timer**.

   NOTE: The **Life class timer** defines the maximum time a connection can be inactive before the *DYNASTAR* automatically disconnects the call.

8. Enter **Y** in the **Process selections** field and press

<return>.

✓ You return to the list of available ports.

9. If you wish to set up security, continue with step 10. If you do not wish to set up security, go to step 17.

NOTE: You do not have to set up security for your IPX-In connections; however, if you do not, anyone will be able to access your equipment.

10. Press **<ESC>** to return to the Configuration menu.

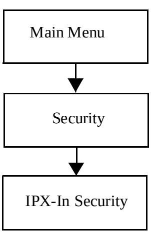
11. Press **<ESC>** again to return to the Main menu.

12. From the Main menu, select **Security**.

✓ The Security Commands menu (Figure 12-15) appears.

13. Select **IPX-In Security**.

✓ The IPX-In Security menu (Figure 12-29) is displayed.




```
                          ***IPX-In Security***
                                              Last changed: 6-6-02  11:26:45


                24 ID strings (9 characters) may be specified.
          They must match ID strings assigned to remote workstations.

            1:                          2:
            3:                          4:
            5:                          6:
            7:                          8:
            9:                          10:
            11:                         12:
            13:                         14:
            15:                         16:
            17:                         18:
            19:                         20:
            21:                         22:
            23:                         24:


________[DynaStar_3614]_________              Process selections (Y/N): Y
To change or add entry, enter new value.      Use <CTRL-D> to delete entry.
Use TAB and CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 12-29 IPX-In Security Menu

14. Enter up to 24 ID strings. These strings must match a valid ID string assigned in the Arconfig file (see the next section, *Configuration of the PC*).

15. When you have entered all the ID strings, enter **Y** in the **Process selections** field and press **<return>**.

✓ You return to the Security Commands menu.

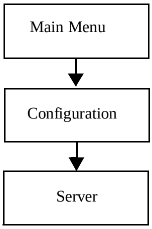
16. Press **<ESC>** to return to the Main menu.

17. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu is displayed.

18. Select **Server**.

✓ The Systemwide Parameters screen (Figure 12-30) is displayed.




```
                    *** Systemwide Parameters***

Server name: DynaStar399c                                                   (47)
Supervisor console herald:     DynaStar Supervisor                          (32)
Dial IP idle timer:            2         (0-disable, 1-254 min, 255-10 sec)
Dial IPX idle timer:           2                   (0-disable, 1-255 min)
Dial Bridge idle timer:        2                   (0-disable, 1-255 min)
B Channel call timeout:        0                  (0-disable, 1-1440 min)
X.25 call set-up timer:        5                              (1-30 min)
XOT Idle Timer                 0                    (0-disable, 1-30 min)
PPP IP prioritization:         0                     (0 - disable, 1-99)
IPX-In preferred File Server:                                       (47)
IPX-Out broadcast address:     399c                                  (8)
Reserved LCNs:                 N                          <CR> to toggle
Exhaustive Routing:            ENDPOINT                   <CR> to toggle
x32 No LCN Drop Timer:         6            <0-disable, 1-12<10 sec>>
Daughter Board Auto-Recover:   Y                          <CR> to toggle


________[DynaStar 399c]________              Process selections (Y/N): Y
Use <TAB> and CURSOR to move fields.   Press ESC to return to previous menu
```

Figure 12-30 System-wide Parameters Screen

19. In the **IPX-In preferred File Server** field, enter the name of the server to be used for IPX-In connections.

20. Enter **Y** in the **Process selections** field and press **<return>**.

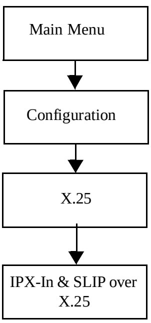
If you are using IPX-In over an X.25 line, perform these additional steps:

1. From the Configuration Commands menu, select **X.25**.

✓ The X.25 Commands menu appears.

2. Select **IPX-In & SLIP over X.25.**

✓ The IPX/SLIP Addresses for Incoming X.25 Calls screen, as shown in Figure 12-31, appears. All ports configured as X.25 are listed in the screen.




```
                    *** IPX/SLIP Addresses for Incoming X.25 Calls***
                                               Last changed: 6-6-02  7:00:45

Port  IPX-In address    SLIP address     IP address mask    Max calls   Idle timer
      (8 HEX digits)   (format x.x.x.x   x = 0 - 255)       (256 max)   (0-60 min)

 5    000000d0           0.0.0.0           0.0.0.0              64          30

________[DynaStar 399c]_______                        Process Addresses (Y/N):Y
Terminate input with <RET>.                     Press ESC to return to previous menu.
```

Figure 12-31 IPX/SLIP Address for X.25 Calls Screen

3. In the **IPX-In address** field, enter the unique IPX-In address for this X.25 connection.

NOTE: Use zeros to represent the host number as you enter the IP address. For example, if you assign the IP address 199.97.52.0, you can give terminals attached to the *DYNASTAR* an IP address in the range 199.97.52.1 to 199.97.52.254.

4. In the **Max calls** field, enter the maximum number of calls that will be allowed over this X.25 connection.

5. In the **Idle timer** field, enter the number of minutes (0-60) to wait before disconnecting a call if there is no traffic on the line.

6. When your entries are complete, enter **Y** in the **Process Addresses** field and press **<return>**.

Configuration of the PC

The following items are required to access an IPX LAN as a remote node via the *DynaStar*:

- A PC with a modem connection or asynchronous access to an X.25 network via an async PAD
- The *DynaStar* Utilities diskette
- The access software provided on the Utilities diskette or a communications package such as ProComm or Crosstalk

Configure the Remote Communications Utility

1. Insert the Utilities disk in the PC and enter the following command:
   A:INSTALL

2. At the PC, change to the REMOTE.WKS directory on the hard drive where the *DynaStar* files are located and enter the following command:
   C:\MENU

✓ The Main menu is displayed.

3. Select **Configure IPX.COM**.

✓ The Arconfig menu is displayed.

4. On the Arconfig menu, select the baud rate, COM port, and the type of modem being used (Hayes compatible or special) to match the settings of your asynchronous connection.

   NOTE: The IP address and user entries are not required.

5. On the same menu, enter the appropriate modem string for your modem.

6. In the **ID String** field on the Edit Shell menu, enter the ID string for the server.

7. To save the configuration, press **<ESC>** and select **YES**.

   NOTE: The driver file can be renamed for different configurations and saved to descriptive names, such as IPX2400 and IPX9600.

Establish an Asynchronous Connection from the PC to the *DYNASTAR*

You now need to establish an asynchronous connection to the *DYNASTAR*. A dial-up communications package is included on the Utilities disk; however, you can use any communications package.

- To use the *DYNASTAR* Access software provided with your equipment, skip to the subsection *Load Server Master List.*

- If you will be using your own communications package, follow the instructions included with that package to dial up the IPX-In port on the *DYNASTAR*. Once a connect message is received, exit the communications package *without* hanging up the line, return to the DOS prompt, and go to the subsection *Load IPX.COM* to continue your configuration.

- If you are accessing the *DYNASTAR* via an X.25 network, simply use the communications package to connect to an asynchronous PAD port. From the PAD port, place an X.25 call using the X.121 address of the X.25 port on the *DYNASTAR*. Once a connect message is received, exit the communications package *without* hanging up the line, return to the DOS prompt, and go to the subsection *Load IPX.COM* to continue your configuration.

Load Server Master List

NOTE: Skip this section if you are not using the ACT Networks communications package.

1. From the *DYNASTAR* Remote Access Utilities menu on the PC, select **Configure Master Server**.

✓ The Access Server Master List is displayed.

2. Enter any name you like for the Access Server.
3. If this is a dial connection, enter a dial-up phone number.
   OR
   If you are connecting over an X.25 PDN, enter the X.121 address of the *DYNASTAR*'s X.25 port.
4. Enter the filename for the connection script under **PDN Name**.

   NOTE: You may need to modify an existing script or create a new one for your environment. You can do this with a standard text editor. Sample script files (ending with the suffix .scr) are located on the Utilities diskette in the REMOTE.WKS directory.

5. When you have completed your entries, press **<ESC>**.

✓ You are prompted to save your entries.

6. Select **Y** and press **<return>** to save them.

Load AsyncGen

1. From the *DYNASTAR* Remote Access Utilities menu on the PC, select the **Configure ASYNCGEN Remote** menu.

✓ The Configure Remote menu is displayed.

2. Select servers to add to the list of accessible servers.

Connect to the Access Server

1. From the *DYNASTAR* Remote Access Utilities menu, select **Run Access Software**.

✓ The Connect to Access Server menu is displayed.

2. Select the server to connect to and press **<return>**. (If only one server has been defined, it is automatically selected for you.)

✓ You are prompted to edit the PAD call number.

3. Press **<return>** to select default values.

✓ You return to the DOS prompt once a connection is established.

Load IPX.COM

1. From the REMOTE.WKS directory on your hard drive, enter the following command:
   C:IPX.COM

Load Netx.COM

1. From the REMOTE.WKS directory on your hard drive, enter the following command:
   C:NETX

✓ A message appears indicating the server you are connected to.

Log In to the Server

1. Change directories to the ?:\LOGIN directory of your server (with ? replaced by the drive where the directory is located), and log in as you would on a direct LAN connection.

   NOTE: To reduce login time, the file LOGIN.EXE in the ?:\LOGIN directory on the server should be copied to the directory C:\REMOTE.WKS on your PC.

■ IPX-OUT

IPX-Out lets Novell Netware LAN users access asynchronous services such as dial-up modems. This function is also available to TCP/IP users communicating over Telnet (see Chapter 13, *Telnet and Async Services*, for more information). A typical use of IPX-Out is illustrated in Figure 12-32.

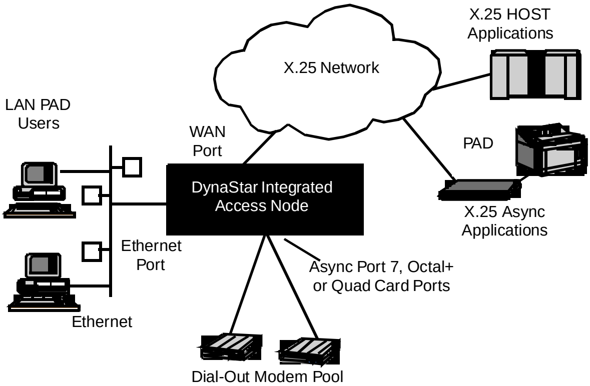


Figure 12-32 IPX-Out Application on the *DYNASTAR*

CONFIGURATION OF THE *DYNASTAR*

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) appears.

2. Select **Port**.

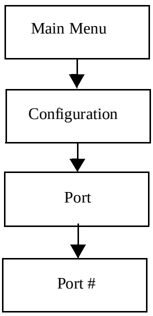
✓ A list of available ports appears.

3. Select the port that you want to configure as IPX-Out and enter that port's number in the **Enter port number** field.

✓ The Port Configuration screen appears.

4. Set the **Port type** to **IPX-Out** or **IPX-In/Out**.

✓ The screen displays the parameters that need to be configured for IPX-Out, as shown in Figure 12-33.




```
                    ***Asynchronous Port Configuration***
                                          Last changed: 6-6-02  11:26:45
 Port: 7  IS-35

 |---  Press <RET> to toggle values  --||--- Type in values.  Max chars shown in ()  ---|
 Port type:    IPX-Out          Port name:       Sync/Async                          (14)


Connection mode:      DIAL
Modem speed:          9600 Baud

Parity:               7-EVEN
Flow control:         NONE          General service name:   IPXOUT                  (8)





________[DynaStar_3614]_________                    Process selections (Y/N): Y
 Use TAB & CURSOR keys to move among fields.   Press ESC to abort command & exit.
```

Figure 12-33 IPX-Out Port Configuration Screen

5. Select the appropriate connection type.
   - **Dial** makes the port appear as a DTE. This selection is used for dial-out connections.
   - **DCE** makes the port appear as a DCE. This selection is used for connection to a terminal.
   - **DTE** makes the port appear as a DTE. This selection is used for connection to a modem.
6. Set the **Modem speed**, **Flow control**, and **Parity**.

   NOTE: The fixed setting for data is 8 bits + 1 stop bit. (Parity is set to 7-EVEN and cannot be changed.)
7. In the **General service name** field, enter a name for IPX-Out connections.

   NOTE: When you are ready to select a driver, the service name you entered will be listed on the General Service menu of your communications package.

8. When you have completed your entries, enter **Y** in the **Process Selections** field and press **<return>**.

✓ You return to the list of ports.

9. If you want to set up IPX-Out security, continue with step 10.
If you do not want to set up security, go to step 16.

NOTE: You do not have to set up security for your IPX-Out connections; however, if you do not, anyone will be able to access your equipment.

10. Press **<ESC>** to return to the Configuration Commands menu.

11. Press **<ESC>** again to return to the Main menu.

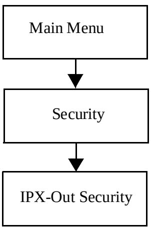
12. From the Main menu, select **Security**.

✓ The Security Commands menu (Figure 12-15) appears.

13. Select **IPX-Out Security**.

✓ The IPX-Out Security menu, shown in Figure 12-34, appears. This menu lists all configured IPX-Out lines and lets you define a password for each one.

14. Enter a password (maximum 16 characters) for each IPX-Out service.



NOTE: Once the passwords are configured, a connection cannot be established unless the user enters a correct password string.

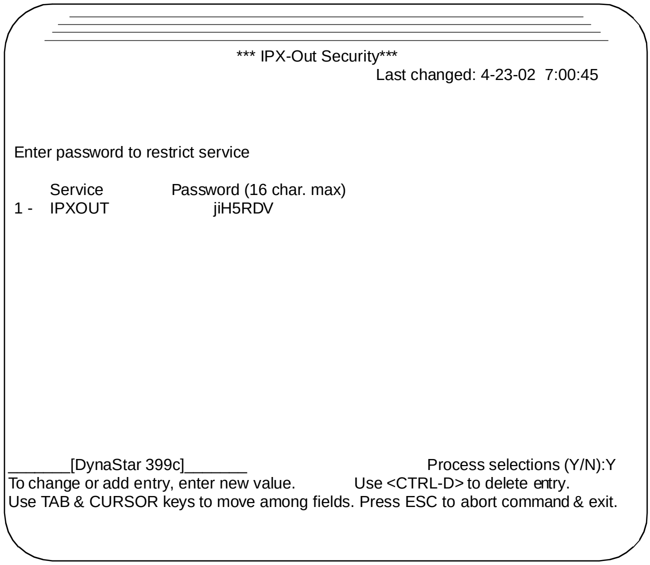


Figure 12-34 IPX-Out Security Menu

15. Enter **Y** in the **Process selections** field and press **<return>**.

✓ You return to the Security Commands menu.

16. Press **<ESC>** to return to the Main menu.

17. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu appears.

18. Select **Server**.

✓ The Systemwide Parameters screen (Figure 12-30) appears.

19. In the **IPX-Out broadcast address** field, enter the IPX number that the *DYNASTAR* will broadcast for the IPX-Out connection.

20. Enter **Y** in the **Process selections** field and press **<return>**.

Configuring the Terminal Connection

To use IPX-Out on the LAN terminal side, you need:

- Novell network drivers (Netware client software)
- Asynchronous communications drivers (such as NCSI or INT14, both provided on the *DynaStar* Utilities diskette)
- A communications program that supports the NCSI driver such as ProComm for Windows, Version 2.0 or higher, or CrossTalk

To configure a terminal connection:

1. Load the Netware client shell.
2. Load the NCSI_WAN (or INT_14) driver supplied on the *DynaStar* Utilities diskette.
3. Load the communications package that supports NCSI or INT_14 drivers.

■ SLIP

SLIP, or Serial Line Interface Protocol, allows remote terminals that require access to your network to establish an asynchronous connection. SLIP receives IP packets and adds a one-character header and a one-character trailer required by the asynchronous protocol. A typical SLIP configuration is shown in Figure 12-35.

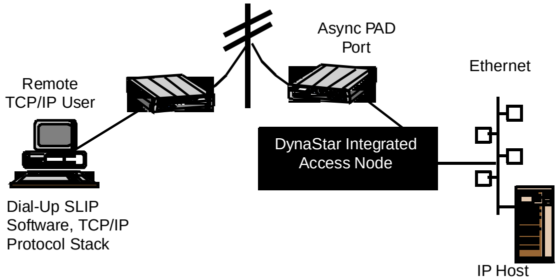


Figure 12-35 SLIP Over a Dial-up Port

CONFIGURATION ON THE *DYNASTAR*

You will need the following to configure SLIP:

- SLIP drivers (TCP/IP protocol stack)
- The TCP/IP applications
- A connection to the *DYNASTAR*, either directly or via a modem

NOTE: Packages such as PC/TCP provide necessary drivers and TCP/IP applications.

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) appears.

2. Select **Port**.

✓ A list of available ports appears.

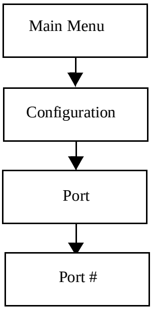
3. Select the port that you want to configure as SLIP and enter that port's number in the **Enter port number** field.

   NOTE: Any asynchronous port can be used for SLIP.

✓ The Port Configuration screen appears.

4. Set the **Port type** to **SLIP**.

✓ The screen displays the parameters that need to be configured for SLIP, as shown in Figure 12-36.




```
                    ***Asynchronous Port Configuration***
                                          Last changed:  6-6-02  11:26:45
 Port: 7  IS-35

 |---  Press <RET> to toggle values  --||--- Type in values.  Max chars shown in ()  ---|
 Port type:    SLIP              Port name:      Sync/Async                          (14)


Connection mode:      DIAL          Modem command:       &Q0S37=9              (25)
Modem speed:          9600 baud     Idle timer:          30    (0-disable, 1-60 min)

Parity:               8-NONE
Flow control:         NONE
                                    IP network address:  0.0.0.0
                                    IP address mask:     0.0.0.0




 ________[DynaStar_3614]_________                  Process selections (Y/N): Y
 Use TAB & CURSOR keys to move among fields.   Press ESC to abort command & exit.
```

Figure 12-36 SLIP Port Configuration Screen

5. Select the appropriate connection mode.

- **Dial** makes the port appear as a DTE. This selection is used for dial-out connections.
- **DCE** makes the port appear as a DCE. This selection is used for connection to a terminal.
- **DTE** makes the port appear as a DTE. This selection is used for connection to a modem.

6. Select the modem speed and type of flow control.

NOTE: The fixed setting for data is 8 bits + 1 stop bit. (Parity is set to 8-NONE and cannot be changed.)

7. In the **IP network address** field, enter the IP network address for SLIP connections.

NOTE: Use zeros to represent the host number in the IP address. For example, if you assign IP address 199.97.52.0, you can give terminals attached to the *DynaStar* an IP address

in the range 199.97.52.1 to 199.97.52.254.
The SLIP network number must be a unique network number.
Subnetting can be used on this network.

NOTE: Remote SLIP terminals must be part of the network.

8. In the **IP address mask** field, enter the IP address mask.

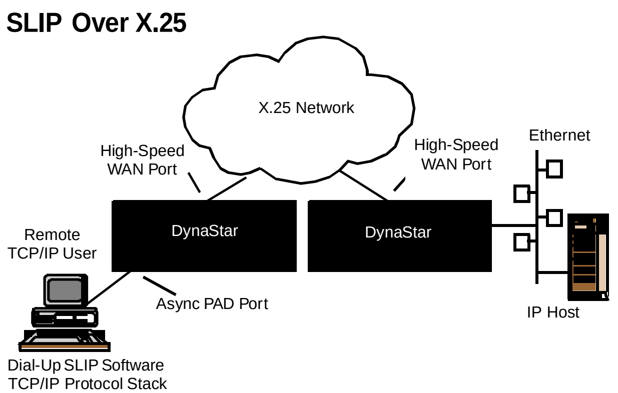


Figure 12-37 SLIP over X.25 Network Configuration

To complete your configuration if you are using SLIP over X.25, as shown in Figure 12-37:

1. From the Configuration Commands menu, select **X.25.**

✓ The X.25 Commands menu appears.

2. Select **IPX-In & SLIP over X.25**.

✓ The IPX/SLIP Address for X.25 Calls screen (Figure 12-31) appears. All X.25 ports are listed.

3. In the **SLIP address** field, enter the unique SLIP address.

   NOTE: You must use zeros to represent the host number as you enter the network number. For example, if you assign the IP address 199.97.52.0, you can give terminals attached to the *DYNASTAR* an IP address in the range 199.97.52.1 to 199.97.52.254.

4. In the **IP address** mask field, enter the IP mask.
5. In the **Max calls** field, enter the maximum number of calls that will be allowed over this X.25 connection.
6. In the **Idle timer** field, enter the number of minutes to wait before disconnecting a call if there is no traffic on the line.
7. When your entries are complete, enter **Y** in the **Process selections** field and press **<return>**.

CONFIGURATION ON THE PC

NOTE: The following procedure assumes that you are using ProComm Plus. If you are using another communications application, the process may vary.

1. Run ProComm Plus or a similar communications application.
2. At thePAD prompt, call the X.25 port on the *DYNASTAR*.
3. Exit from ProComm Plus *without* hanging up.
4. Run the SLIP drivers.
5. Ping the Ethernet port to confirm connection.

■ VIRTUAL PRIVATE NETWORKS

The Virtual Private Network (VPN) allows organizations to use service provider networks for secure exchanges with remote offices, vendors, and partners. VPNs encrypt transmissions using key exchanges, hashing, and encryption algorithms.

The *DYNASTAR* implementation of the VPN conforms to IPSec RFC2401 and provides VPN solutions for both site-to-site (router-to-router) and remote access VPN deployments. This is an optional feature on the *DYNASTAR* that requires a software key for activation.

IPSec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and set up any cryptographic keys required to provide the requested services. IPSec can be used to protect one or more “paths” between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

VPN CONFIGURATION

To configure a VPN on the *DYNASTAR*, follow the procedure below.

1. From the Main menu, select **Configuration**.

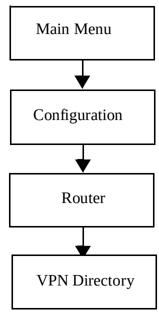
✓ The Configuration Commands menu (Figure 3-11) appears.

2. From the Configuration Commands menu, select **Router**.

✓ The Router Commands menu (Figure 12-2) appears.

3. From the Router Commands menu, select **VPN Directory**.

✓ The Configured VPN Names screen (Figure 12-38) appears.



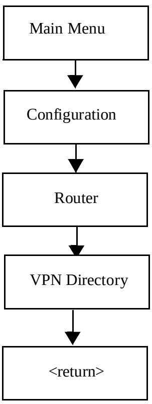

```
                         ***Configured VPN Names***
                                         Last changed:  6-6-02  11:26:45





                           Enter Feature Key:


 ________[DynaStar_3614]_________
To add entry, just press <RET>              Press ESC to return to previous menu
To edit entry, enter service # <RET>           Cursor up/down for more entries
To delete entry, enter service # <CNTL-D>  NOTE: Delete takes place immediately
```

Figure 12-38 Configured VPN Names Screen

> **NOTE:** If **Enter Feature Key** appears at the bottom of the screen, the VPN feature has ***not*** been enabled on this device. Please call *DYNASTAR* technical support for assistance.

4. Press **<return>** to add a new entry.

✓ The VPN Configuration screen (Figure 12-39) appears.




```
                              ***VPN Configuration***
                                          Last changed:  6-6-02  11:26:45

VPN Name:                                                              (15)
Dest. IP address:         0.0.0.0
IKE Encryption:
IKE Hash:                 MD5
IKE Lifetime:             0                    (1-9999 Days, 0 = Unlimited)
IKE Setup:                MAIN
Key Exchange:             Private
Private Key1:                                                      (16 Hex)
Diffie-Hellman:           1536-bit
Encapsulation:            TUNNEL
IPSec Protocol:           ESP
IPSec Lifetime:           0                    (1-9999 Days, 0 = Unlimited)
IPSec Hash:               MD5
IPSec Encryption:



 ________[DynaStar_3614]_________              Process selections (Y/N): Y
Use <CTRL-D> to delete entry                 <RET> to toggle or type value
Use <TAB> and CURSOR to move fields    Press ESC to return to previous menu
```

Figure 12-39 VPN Configuration Screen

5. Complete parameters as required. Parameters and their values are explained in Table 12-9.

6. When you have completed your entries, enter **Y** in the **Process selections** field and press **<return>**.

✓ You return to the Configured VPN Names screen (Figure 12-38). Your newly configured VPN is listed on the screen.

7. You now need to set up IP filtering to define what traffic and what types of applications will use the VPN. Press **ESC** three times to return to the Main menu.

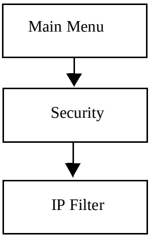
✓ The Main menu appears.

8. From the Main menu, select **Security**.

✓ The Security Commands menu (Figure 12-15) appears.

9. From the Security Commands menu, select **IP Filter**.

✓ The IP Filter Table (Figure 12-40) appears.




```
                         ***IP Filter Table***
                                        Last changed:  4-23-02  11:26:45
  Class   Source IP   Mask      Destination IP   Mask    FTP  TEL  PNG   WWW   OTH
(Toggle) (Address)   (# Bits)  (Address)       (# Bits)             (Toggle)
 1:D        *.*.*.*      *        101.1.1.64        *     VPN1 VPN1 VPN1 VPN1 VPN1
 2:
 3:
 4:
 5:
 6:
 7:
 8:
 9:
 10:
 11:
 12:
 13:
 14:
 15:
Default Filter Action:   FTP   TEL   PNG   WWW  OTH
                         FWD  FWD  FWD  FWD   FWD

 ________[DynaStar_3614]_________                Process IP Filter table (Y/N): Y
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 12-40 IP Filter Table Showing VPN Configuration

10. Complete the table as required by your network. (See *IP Filtering* earlier in this chapter for detailed information about the table.)

The filter table in Figure 12-40 above shows the configuration of a filter that will route ALL source IP addresses to remote address 101.1.1.64. All applications (FTP, Telnet, PNG, WWW, and Other) will be sent over VPN1. This filtering configuration would discard any inbound traffic from 101.1.1.64 that is NOT received over the VPN.

Table 12-9 VPN Configuration Parameter s

Parameter	Description	Values
VPN Name	A name to identify the VPN. This name does not need to match the name at the distant location, but this is recommended for continuity	Max 15 alphanumeric characters
Dest. IP address	The IP address of the remote device.	0.0.0.0 - 255.255.255.255 (4 bytes) Default = 0.0.0.0
IKE Encryption	Type of Internet Key Encryption encryption to be used. Null is implemented as described in RFC2401. DES is implemented as described in RFC2405. 3DES, or Triple DES, is described in ANSI X9.52-1998.	Null DES 3DES
IKE Hash	The method used to guarantee the integrity of your data. MD5 is defined in RFC1321. SHA-1 is described in FIPS180-1.	MD5 (default) SHA-1
IKE Lifetime	Sets the lifetime of an IKE security Association (SA). Set to zero for unlimited, or in full day increments up to 9999 days. If the initiator and responder Lifetime values are not the same, the shortest duration will be adopted at both ends.	0 (= unlimited) 1- 9999 days 0 is the default
IKE Setup	Main is a 6-step (3 round trip) process that provides identity protection by encrypting the identities of the peers. Aggressive mode is somewhat faster than Main, but it does not protect the identities of the communicating parties.	Main (default) Aggressive (not currently supported)

Table 12-9 VPN Configuration Parameter s(cont.)

Parameter	Description	Values
Key Exchange	Manner in which keys are exchanged.	Private (default) Public (not currently supported)
Private Key1	The key to exchange when Private is selected above. It is required when Private is selected.	Max 16 hexadecimal characters
Diffie-Hellman	This is a means for two parties to agree upon a shared secret in such a way that the secret is unavailable to eavesdroppers. The secret can then be converted into cryptographic keying material for other algorithms.	
Encapsulation	Type of encapsulation used. Only tunnel mode is available at this time.	Tunnel
IPSec Protocol	The protocol format used. The protocol formats for IPSec’s Authentication Header (AH) and IP Encapsulating Security Payload (ESP) are independent of the cryptographic algorithm, although certain algorithm sets are specified as mandatory for support in the interest of interoperability. The AH protocol defines methods of establishing the identity of the message originator and ensures that the transmitted data has not been tampered with. ESP protocol provides the same functions as the AH protocol but additionally defines encryption methods for the data.	AH ESP (default)

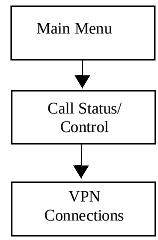
Table 12-9 VPN Configuration Parameter s(cont.)

Parameter	Description	Values
IPSec Lifetime	Sets the lifetime of an IPSec Security Association (SA). Set as zero for unlimited or in ful day increments up to 9999 days. If the initiator and responder Lifetime values are not the same, the shortest duration will be adopted at both ends.	0 (= unlimited) 1- 9999 days 0 is the default
IPSec Hash	The method used to guarantee the integrity of your data. MD5 is defined in RFC1321. SHA-1 is described in FIPS180-1.	MD5 (default) SHA-1
IPSec Encryption	Type of encryption to use. Only available if IPSec Protocol is set to ESP. Null is implemented as described in RFC2401. DES is implemented as described in RFC2405. 3DES, or Triple DES, is described in ANSI X9.52-1998.	Null DES 3DES

VPN Status

VPN status is given in the VPN Connection Status screen. This screen is accessed from the Call Status/Control screen and is shown in Figure 12-41.

The first entry (address 0.0.0.0) is looking for VPN setup attempts and should never change. If you clear this entry with CTRL-D, no VPNs can be set up until the next warm start. Subsequent entries in the table show setups for each configured VPN. Entries on this screen are explained in Table 12-10.




```
                         ***VPN Connection Status***

Dest. IP Addr. Phase 1        Phase 2    Proto.   SPI        Sequence
               State          State                          TX                RX

0.0.0.0        LISTENER       RESRVD                         0                 0
1.1.1.1        CONNECTED      VPN UP     ESP      13AB3403   103478            1024534






 ________[DynaStar_3614]_________
Press <RET> for update                               Cursor up/down for more entries
Press <CNTL-D> to clear call                     Press ESC to return to previous menu
```

Figure 12-41 VPN Connection Status Screen

Table 12-10 VPN Status Parameters

Parameter	Description	Values
Dest IP Addr	The destination IP address that the VPN tunnel connects to.	0.0.0.0 - 255.255.255.255
Phase 1 State	The state of the phase 1 Internet Key Exchange (IKE) setup.	See Table 12-11.
Phase 2 State	The state of the phase 2 IKE setup.	See Table 12-11.
Protocol	The method of encapsulation.	AH (authentication header) ESP (encapsulating security protocol)
SPI	A unique identifier for each connection.	Usually a random number, displayed in hexadecimal

Table 12-10 VPN Status Parameters (cont.)

Parameter	Description	Values
Sequence TX/RX	The current sequence number in each direction. This also indicates how many frames have been sent and received since the last phase 2 rekey-ing occurred.	Decimal number

Table 12-11 Phase 1 and Phase 2 States

State	Description
Phase 1 States	
VPN IDLE	No setup attempt is pending (not normally seen)
PRE-SETUP	Waiting for timeout to initiate setup
AGGR INIT	Initiated aggressive mode setup
AGGR RESP	Aggressive mode response sent
MAIN SA IN	Main mode security association initiated
INIT RX	Main mode setup message received
MAIN SA RE	Main mode security association response sent
MAIN KEY IN	Main mode key setup set
MAIN KEY WT	Waiting for key response (this can take seconds depending on the processor speed at the other end)
MAIN KEY RE	Main mode key response sent
MAIN ID IN	Main mode ID message sent
MAIN ID RE	Main mode ID response sent
CONNECTED	Phase 1 setup is complete
Phase 2 States	
QK SETUP IN	Phase 2 setup (quick mode) initiated

Table 12-11 Phase 1 and Phase 2 State s(cont.)

State	Description
QK SETUP WT	Waiting for phase 2 response (can take seconds depending on the processor speed at the other end)
QK SETUP RE	Phase 2 response sent
NEW GRP IN	New group request initiated
VPN UP	VPN is up and sending data

TELNET AND ASYNC SERVICES

INTRODUCTION

Telnet is a terminal emulation application that allows you to log into a remote host. The Telnet application can access any host system that has implemented the TCP/IP protocol and a Telnet server package.

DYNASTAR CAPABILITIES

The *DYNASTAR* provides an internal Telnet server that allows async users connected to the *DYNASTAR* directly, through a LAN, or across an X.25 network to use the Telnet application remotely. The async terminals do not need to implement any part of the TCP/IP stack or the Telnet application locally.

Likewise, the *DYNASTAR* can provide asynchronous service to terminals that support the TCP/IP protocol and the Telnet application. This allows Telnet clients to placePAD calls across an X.25 network and provides access to asynchronous dial-out modems.

TELNET APPLICATIONS ON THE *DYNASTAR*

The Telnet Supervisor application allows Telnet users to connect to a *DYNASTAR* supervisor. Full management capabilities are provided via this connection.

The IP Dial-out application allows Telnet users to dial out from their LAN using *DYNASTAR* X.25 or async ports. The Telnet/TCP/IP portion of the messages are terminated at the *DYNASTAR*.

The Telnet Terminal application allows remote users of asynchronous terminals to access Telnet facilities of TCP/IP hosts. Incoming data from a terminal is forwarded to the Telnet Host in Telnet/TCP/IP packets. The Telnet/TCP/IP

portion of the messages transmitted by the host to the terminal are terminated at the *DYNASTAR*.

The X.25-Out and X.25-Out Stream applications allow a Telnet client to reach a remote X.25 device. The X.25-In application allows a remote X.25 user to reach a TCP/IP device.

The embedded data contained within the Telnet/TCP/IP packet is forwarded via an X.25 port in an X.25 packet or via an async port as asynchronous data. Incoming data is forwarded to the Telnet user in Telnet/TCP/IP packets.

■ ESTABLISHING TELNET SESSIONS FROM PAD PORTS

Async ports configured as PADs are able to support both X.25 PAD calls and calls to Telnet hosts. The initial connection to the port receives the PAD prompt (*).

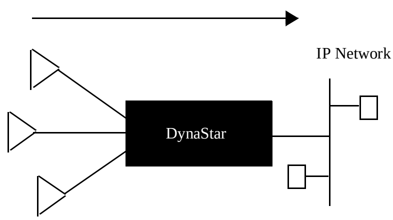


Figure 13-1 Telnet Sessions from PAD Ports

To begin a Telnet session:

1. First, establish an async PAD connection to the *DYNASTAR*.

   NOTE: For information on configuring the PAD connection, see Chapter 7.

2. Once an async terminal connection has been established to the *DYNASTAR*, at the PAD prompt (the default prompt is *), type:
   telnet <return>

✓ The port switches from PAD operation to Telnet operation, and the PAD prompt is replaced by the Telnet>

prompt. The Telnet> prompt indicates that the terminal is in Telnet command mode and is able to accept Telnet commands.

To display a menu listing the current settings of the Telnet service and the Telnet commands:

1. At the Telnet> prompt, type:
?<return>

✓ A screen similar to Figure 13-2 is displayed.

The system returns the summary of the current settings for the Telnet Client:

Echo = Remote, data = 7 Bit, End of Line = CRLF

The commands required to change Telnet settings are listed on the screen. For more information on these commands, see the section *Telnet Commands* later in this chapter.

2. At the Telnet> prompt, enter the IP address of the Telnet server you want to connect to, followed by the -q option to ensure that the call hangs up when completed. For example:
Telnet> **192.100.100.14 -q <return>**

NOTE: Additional Telnet commands are available after a session is established (see example in Figure 13-3). You can view these options by typing **?** at the Telnet prompt. These options are described in the section *Telnet Commands*.

```
>?
Client settings:
Echo = Remote, Data = 7 Bit, End of Line = CRLF


Client establish connection options:
-D    7/8 bit data                          default 7
-E    Terminal/Local/Remote Echo            default R
-F    Force CR to Cr/crLf/crNull            default L
-K    Kill Telnet session
-L    Local control char default ] or ^]
-N    No check for local mode access
-P    Profile number/Profile name
-R    Raw TCP connection
-T    Terminal-Type                         default NVT
```

Figure 13-2 Telnet Commands Available Prior to Connection

```
Telnet>?
Client settings:
Echo = Remote, Data = 7 Bit, End of Line = CRLF

Client session options:
-A    Abort Output
-B    Break
-C    Close connection
-D    7/8 bit data                          default 7
-E    Terminal/Local/Remote Echo            default R
-F    Force CR to Cr/crLf/crNull            default L
-I    Interrupt Process
-K    Kill Telnet session
-L    Local control char default ] or ^]
-N    No check for local mode access
-P    Profile number/Profile name
-T    Terminal-Type                         default NVT
-X    Exit options
-Y    Are You There

Telnet> -X
```

Figure 13-3 Telnet Commands Available During aTelnet Session

TERMINATING A CONNECTION

To terminate the Telnet connection and exit the Telnet command mode:

1. Enter **<Ctrl-]** to get to the Telnet> prompt. Then enter **-K**

✓ The *DYNASTAR* disconnects the TCP connection if the user terminates the connection with the Telnet Host or if the device attached to the async port drops its data set signal.

NOTE: It is always a good idea to use the -K command to terminate calls.

■ ESTABLISHING INBOUND TELNET CLIENT SESSIONS VIA X.25

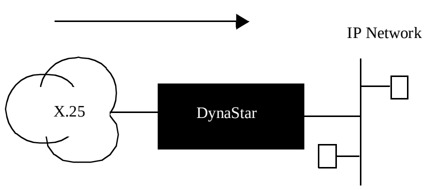


Figure 13-4 Inbound Telnet Connection via X.25

Figure 13-4 illustrates an inbound Telnet client session. The user is establishing a Telnet session with an IP host through an intermediate X.25 network. In this configuration, the user first establishes an X.25 connection to the *DYNASTAR*, and a Telnet session is established through a LAN port on the *DYNASTAR* to the IP host.

You can establish a Telnet session for this type of configuration manually or automatically. The following procedure explains how to establish a manual connection. Automatic connections can be established as described in the next section.

MANUAL CONNECTION

Before performing this procedure, you must first have configured an X.25 port on the *DYNASTAR*. For information, see Chapter 6, *The X.25 Application*.

To connect to a Telnet client via X.25:

1. First, establish a connection to the *DYNASTAR* by entering the X.121 address that has been assigned to the X.25 port on the target *DYNASTAR*.
2. Press **<return>** twice. (The double carriage return allows the *DYNASTAR* software to automatically establish the baud rate and parity to be used for the session.)

✓ The *DYNASTAR* responds by issuing the Telnet> command mode prompt. An X.29 command is sent to the remote PAD, setting all X.3 parameters except parameter 4 to 0. Parameter 4 is set to 1.

NOTE: The user can change this profile with a **-P** command as described in the *Telnet Commands* section. X.3 parameters can also be adjusted individually by the user.

3. Initiate a telnet session as required by your network.

AUTOMATIC CONNECTIONS

You can configure an automatic Telnet connection by configuring an X25-In async service and entering the IP address and socket number of the destination Telnet device. The X.121 address of the service entry must be unique.

When you establish an X.25 connection to the X.121 address you entered on the Async Services menu for the Telnet service, the *DYNASTAR* automatically and transparently connects you to the remote IP host.

For more information, see the *X25-In* and *Configuring Async Services* sections later in this chapter.

NOTE: For a list of Telnet commands or for information on exiting Telnet, see the previous section, *Establishing Telnet Sessions from PAD Ports*.

■ ESTABLISHING OUTBOUND TELNET CLIENT CONNECTIONS

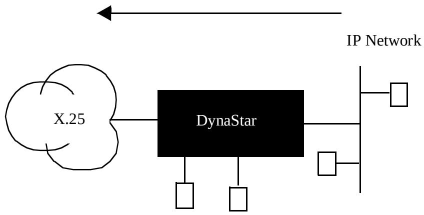


Figure 13-5 Outbound Telnet Client Configuration

Telnet users are able to Telnet into a *DYNASTAR* to make outbound connections to X.25 devices, local or remote *DYNASTAR* async ports, or to the *DYNASTAR* Supervisor port as long as an IP address has been configured for the *DYNASTAR* in a previous session. Figure 13-5 illustrates an outbound Telnet client connection. The following sections describe these three types of outbound connections.

NOTE: For information on configuring IP addresses, see Chapter 12, *The IP/IPX Router Application*.

Telnet users are able to Telnet into a *DYNASTAR* to make outbound connections via X.25 and async ports and to connect to the Supervisor as long as an IP address has been configured for Telnet on the *DYNASTAR* in a previous session. For information on configuring IP addresses, see Chapter 12, *The IP/IPX Router Application*.

To initiate a connection to the *DYNASTAR* from a Telnet client, use the procedure required on the client to access the IP address of the *DYNASTAR*.

X.25 OUTBOUND CONNECTIONS

Telnet users can make outbound X.25 connections manually or automatically.

NOTE: To configure outbound Telnet client connections over X.25, you must previously have configured a working X.25 trunk. See Chapter 6, *The X.25 Application*, for more information on configuring X.25.

MANUAL CONNECTION

1. From the Telnet> prompt, enter the IP address of the *DYNASTAR*.

✓ The *DYNASTAR* returns a listing of available services as shown in Figure 13-6.

NOTE: For security purposes, you may wish to configure your system to bypass this menu. See Chapter 3, *The Supervisor*, for more details.

```
DynaStar_f00001 services

     1    Console        f00001
     2    X25PDN         PAD60

     Enter service selection: 4
     *
```

Figure 13-6   Available Services

2. Type the number listed in front of the X25 PDN service on the menu and press **<return>**.

✓ You are connected to a virtual PAD port. (You appear to be directly attached to an X.3 PAD.)

3. Enter the X.121 address of the remote device and press **<return>**.

✓ The outbound X.25 connection is established.

AUTOMATIC CONNECTION

By configuring an Async Services entry for X25-Out, Telnet users can be connected automatically. In the Async Services entry, enter the IP address (and socket if required) and the X.25 address of the remote device. When a user Telnets to this IP address, the *DYNASTAR* transparently establishes a connection to the remote device. See the section *Connections Defined on the Async Services Menu* later in this chapter for more information on configuring Async Services parameters.

ASYNCHRONOUS CONNECTION

Assuming that you have properly configured async ports and have assigned an X.121 address to the *DYNASTAR*, you can establish Telnet connections to local or remote async ports. Async Services entries handle this function. Configure a service for X25-Out. Enter the IP address (and socket if required) of the *DYNASTAR* and enter the X.121 address of the async port you wish to connect to.

NOTE: For more information on async port parameters, see Chapter 7, *The PAD Application*.

NOTE: Socket values allow you to use only one IP address per *DYNASTAR* while allowing a wide range of async ports to be selected. Each async service can handle one async connection or many async connections. To configure an async rotary, simply enter the same X.121 address for multiple async ports.

To initiate a connection from the virtual PAD of another *DYNASTAR*:

1. At the PAD prompt (the default prompt is *), type **telnet <return>**.

✓ The *DYNASTAR* responds by issuing the Telnet> command mode prompt.

2. At the Telnet> prompt, enter the IP address of the Telnet server you have configured on the *DYNASTAR*, followed by the -q option to ensure that the call hangs up when completed. For example:
   Telnet> **192.100.100.14 -q <return>**

SUPERVISOR CONNECTION

To Telnet to the Supervisor Console:

1. From the Telnet prompt, enter the IP address of the *DYNASTAR*.

✓ The *DYNASTAR* returns a listing of available services as shown in Figure 13-6.

NOTE: The Console service will not appear in the list of available services if it is in use.

NOTE: For security purposes, you may wish to configure your system to bypass this menu of available services. However, it is still possible to log into the supervisor using mnemonics. See Chapter 3, *The Supervisor*, for more details.

2. Enter **1 <return>**.

✓ You are connected to the Supervisor Console, and the Supervisor Log In menu (Figure 13-7) is displayed.

```
DynaStar Supervisor

DynaStar 500
Software Version number - 6.07.3

Copyright (c) 1990-2002

Press ESC to exit Supervisor
To get back into Supervisor, type 9999 <RET>

Enter Password:
```

Figure 13-7 Login Menu for the *DYNASTAR 500*

SESSION CAPACITY

Up to 255 virtual sessions are available on the *DYNASTAR* for Async-Telnet and Telnet-Async communication.

■ TELNET COMMANDS

The user is able to change certain Telnet settings by issuing Telnet commands while in the Telnet Command mode without disconnecting the current Telnet connection. It is possible to return to the Telnet command mode after a Telnet connection is made by typing the control characters defined to enter local command mode. The default is CNTRL-]. The character is defined by the Telnet command -L. When you enter local command mode, the options listed in Table 13-1 are displayed. The table specifies which settings can be changed during a Telnet connection.

Table 13-1 Telnet Command Descriptions

Command	Example/Description	Options
?	Telnet>? Displays current settings and options. Used before and during connection.	None
IP Address	Telnet>192.100.100.14 Places a Telnet call to the specified address. Used before connection.	None
Socket Number	Telnet>192.100.100.14 24 Adds port/socket number to the IP address (Socket #24 in example). A space separates the IP address from the socket number. Used before connection. Caution: Do not use the IP address of the Ethernet Port with the default socket (23), as this will lock you out of the Console port. Avoid using Socket 1998, which is reserved for the XOT function. For information on XOT, see Chapter 6, *The X.25 Application.*	1-65535 Default = 23
-A Abort	Telnet>-A Sends an Abort Output command to the Telnet host. The process that is running on the host will run to completion but will stop transmitting to the Telnet Client. Used during connection.	None
-B Break	Telnet>-B Sends a break to the Telnet Host. Used during connection.	None
-C Close	Telnet>-C Closes current Telnet connection and returns a Telnet> prompt. Used during connection.	None

Table 13-1 Telnet Command Descriptions (cont.)

Command	Example/Description	Options
-D Data Bits	Telnet>-D 8 Sets the Telnet connection for 7 or 8 data bit operation. Used before and during connection. There *must* be a space between the -D and the number.	7, 8 Default = 7 bits
-E Echo	Telnet>-E R Controls the echo function for the connection. Options are: Terminal: Characters entered at the terminal are sent to the host and are displayed on the screen by the terminal. Local: Characters entered at the terminal are sent to the host and are returned (echoed) by the *DYNASTAR* for display on the screen by the terminal. Remote: Characters entered at the terminal are sent to the host and are returned (echoed) by the host for display on the screen by the terminal. Used before and during connection.	T (Terminal) R (Remote) L (Local) Default = R
-F Force CR	Telnet>-F N Defines the second character that is sent along with a Carriage Return character. Used before and during connection.	C (CR alone, CR Sent) L (Line Feed, CRLF Sent) N (Null, CRNull Sent). Default = L
-H *xxxx* (where *xxxx* are two hexa-decimal bytes that will be sent as a Telnet command)	Will Suppress Go Ahead For example: -H FB03 would send 0xfb (251 decimal parameter code for AWill@) followed by 03 (value for suppress go ahead).	Can be entered at server only.

Table 13-1 Telnet Command Descriptions (cont.)

Command	Example/Description	Options
-I Interrupt	Telnet>-I Sends an interrupt command to the Telnet host. Normally, this stops the process that is running on the host but does not disconnect the connection. Used during connection.	None
-J	Telnet> -J Sets up 8-bit transfer with no negotiation of Telnet parameters. Can be entered only on Async Services menu for Outbound Services. Used during connection.	None
-K Kill	Telnet>-K Ends the Telnet session and returns the *PAD prompt. Used before and during connection.	None
-L Local	Telnet>-L x Defines the character the user will enter to display the Telnet prompt when in a Telnet session. This allows the user to change Telnet options. For example, entering ^] from the terminal causes the system to respond with Telnet> -X, which clears the Telnet> prompt and returns to the Telnet connection. Used before and during connection.	] entered as ^]
-LF	Remove line feeds from the data stream.	Can be entered at server only.
-M	Enables Modbus over TCP protocol.	
-N No Escape	Telnet>-N Disables the ability to escape from a Telnet connection to the Telnet> facility menu with the ^] command. This setting is required for transparent operation with systems that could include an escape sequence (e.g. ^]) in the data stream. Used before and during connection.	None

Table 13-1 Telnet Command Descriptions (cont.)

Command	Example/Description	Options
-NULL	Remove any NULL characters that follow carriage returns in the data stream.	Can be entered at server only.
-P	Telnet>-P 90 Used to set a local port's X.3 profile or to call an X.29 command to set a remote port's X.3 profile. Used before and during connection.	Name or number of any profile defined on the PAD Profiles screen. (See Chapter 7, *The PAD Function*, for more information on PAD Profiles.) Default = Null
-Q	Telnet>192.100.100.14 -Q Clears the X.25 call when a Telnet session ends. (Causes the *DYNASTAR* to clear an X.25 call if it receives a TCP clear.) Can be entered on Async Services menu or directly on Telnet command line. Used before connection.	None
-R Raw	Telnet>-R Raw mode. Allows for raw data transfer. Creates a TCP connection without any Telnet parameters. If you are using raw mode, the only Telnet commands that have effect are -K and -Q.	Can be entered at either client or server.
-T Terminal	Telnet>-T VT100 Allows the user to signal to the host the type of terminal in use. This is a string that is passed to the host. The string can be up to 40 characters long. Embedded spaces are not allowed. (This is not a command to configure emulation in the *DYNASTAR*.) Used before and during connection.	Any terminal type supported by the Telnet client Default = NVT (network virtual terminal)

Table 13-1 Telnet Command Descriptions (cont.)

Command	Example/Description	Options
-T N	Won't Negotiate Terminal Type. That is, the server sets the terminal type. (By default, the command Do Negotiate Terminal Type is sent.)	Can be entered at server only.
-W	Invitation to Clear. When the Telnet session is cleared, it uses an X.29 Invitation to Clear packet to terminate the X.25 portion of the call.	Can be entered at either client or server.
-X Exit	Telnet>-X Exits the Telnet> facility menu and returns to the Telnet connection. Used after connection.	None
-Y Hello	Telnet>-Y Sends an "are you there" message to the Telnet host. Used during connection.	None

Sample Commands

A space must be entered between each command and option. Commands are not case sensitive. A Carriage Return executes the command.

Commands can be concatenated on the Telnet> command line in any order. Separate each command with a space. Here are several examples of valid Telnet commands.

Telnet>**192.100.100.14**
All Defaults

Telnet>**192.100.100.14 24**
Specify Socket #24

Telnet>**192.100.100.14 -T VT100**
Specify VT100 Terminal

Telnet>**-E L -T VT320 -D 8 192.100.100.14**
Specify local echo, VT320 terminal, and 8 data bits

Telnet>**-N**
Disables escape from a Telnet connection to the Telnet> prompt

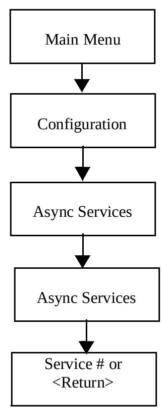
Telnet>**-X**
Exits the Telnet> facility menu

■ CONNECTIONS DEFINED ON THE ASYNC SERVICES MENU

The purpose of the Async Services menu (Figure 13-8) is to facilitate delivery of encapsulated asynchronous data to or from a TCP/IP network, frequently through an intermediate X.25 network. You can configure the Async Services menu with appropriate information for establishing several different connections by naming a configuration and then specifying service type, network addresses, and, when appropriate, Telnet and X.3 parameters to be used.

```
                         *** Async Services ***


          Service name:        DynaStar7bit                (15)
          Service type:        TELNET
          IP Address           192.100.100.14
          Socket Number:       23
          X.121 address:       30077                   (15 BCD)
          X.3 Profile:         87 (12) TELNET        (Name or #)
          Telnet command:      -E R -D 8                   (23)
          CUG:                                           (0-99)
          Call UserData:                                   (32)
          TCP Idle Timer:      0             (1-255 min., 0=OFF)




_________[DynaStar_3df2]__________             Process selections (Y/N): Y
Use <CTRL-D> to delete entry.              <RET> to toggle or type value
Use TAB & CURSOR keys to move fields.      Press ESC to return to previous menu
```

Figure 13-8 The Async Services Screen



In Figure 13-8, the call to the X.121 address 30077 will connect with the *DYNASTAR*'s Telnet facility. It will connect with

Telnet host 192.100.100.14, directing the Telnet host to echo (-E R). This call sequence notifies the host that the data is in 8-bit format.

ASYNC SERVICE TYPES

Several types of service are available on the Async Services menu: PAD, Telnet, IPX-In, SLIP, X25-In, X25-Out, and X25-Out Stream, X25-Out LCN0, and Multicast. The type of service selected determines how the *DYNASTAR* uses the various screen parameters in establishing a connection. Service types are summarized in the following paragraphs.

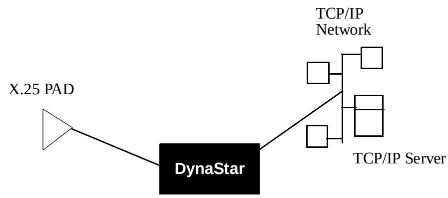


Figure 13-9 Telnet application

PAD. The PAD feature available on this menu has been replaced by the MnemonicTable. For more information on the Mnemonic Table or other PAD capabilities and parameters, see Chapter 7, *The PAD Function*.

TELNET. Telnet service, when configured on the Async Services menu, receives asynchronous data transported over X.25 and delivers it to an IP destination. Figure 13-9 shows a typical application of the Telnet service. When it receives a call request from the PAD, the *DYNASTAR* checks the X.121 address and CUG (if present) against async service configurations. (If a CUG is defined for the async service, both the X.121 address and CUG in the call request must match.) If a match is found for a Telnet service, a connection is established to the IP address and socket entered on the same menu. The *DYNASTAR* strips the data out of X.25 frames and delivers it as an unformatted stream of data to the TCP/IP network. In the opposite direction, the *DYNASTAR* strips the TCP/IP frame headers and delivers the data as X.25 frames.

NOTE: You must already have configured an IP port on the *DYNASTAR*. For more information, see Chapter 12, *The IP/IPX Router Application*.

NOTE: Standard Telnet service does not maintain packet boundaries as data is delivered to the TCP/IP network. However, some applications need complete messages to be identified so that they can be processed properly. To rebuild complete messages, the *DYNASTAR* adds a header to frames sent to IP and syncs on and strips the header on frames coming from IP. for X.25-Out services.
Frames received from X.25 are accumulated based on M-bits and the length of the total message is calculated. The header is then applied and the result forwarded to the IP host. Frames received from IP are scanned for the sync bytes. When these are found, the message length is pulled out and used to rebuild the complete message.

IPX-IN. When IPX-In is configured as an Async Service, the *DYNASTAR* receives IPX data transported in X.25 frames and delivers it to a Novell network destination.

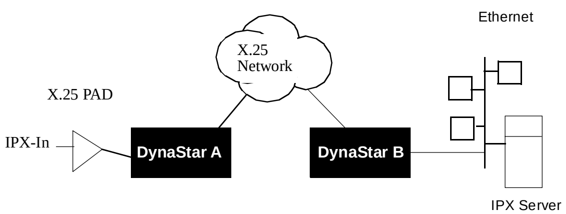


Figure 13-10 IPX-In application

Figure 13-10 shows a typical IPX-In application. In this example, the PAD is set up for transparent operation. IPX data is received by the PAD and routed by *DYNASTAR A* over an X.25 trunk to *DYNASTAR B*. *DYNASTAR B* then checks the Async Services entries before routing the data.

If a call request received from the PAD contains the same X.121 address as an IPX-In service configured on an Async Services menu, *DYNASTAR B* accepts the call and strips the

data out of the X.25 frames sent by the PAD. The *DYNASTAR* then sends the data as an IPX data stream to the Novell network number contained in the data, based on information in the *DYNASTAR*'s IPX routing table.

NOTE: You must already have configured an IPX-Out port on the *DYNASTAR* as well as IPX routing tables. For more information, see Chapter 12, *The IP/IPX Router Application*.

SLIP. SLIP service, when configured on the Async Services menu, allows SLIP data to be transported over X.25 and delivered to an IP destination. Figure 13-11 shows a typical SLIP application. As in the previous example, the PAD is set up for transparent operation. SLIP data is received by the PAD and routed by *DYNASTAR A* over an X.25 trunk to *DYNASTAR B*.

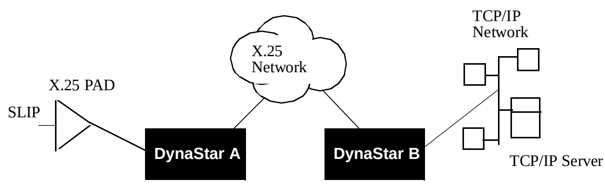


Figure 13-11 SLIP application

When *DYNASTAR B* receives an X.25 call request containing the same X.121 address as a SLIP service configured on an Async Services menu, the call is accepted. As data is received from the PAD, it is stripped out of X.25 frames. The *DYNASTAR*'s IP router then sends the data as a TCP/IP data stream to the IP address contained in the SLIP data.

NOTE: You must previously have configured an IP port as well as IP routing tables. For more information, see Chapter 12, *The IP/IPX Router Application*.

X25-IN. Figure 13-12 shows a typical X25-In application. In the example, async data from the PAD is sent to the *DYNASTAR* over an X.25 line. When it receives a call request from the PAD, the *DYNASTAR* checks the X.121 address and CUG (if present) against async service configurations. (If a CUG is defined for the async service, both the X.121 address and CUG in the call request must match.) If a match is found for an X25-In service, the X.25 frame information is stripped off and the data is transmitted as an IP data stream to the IP address and socket number specified on the same Async Services menu.

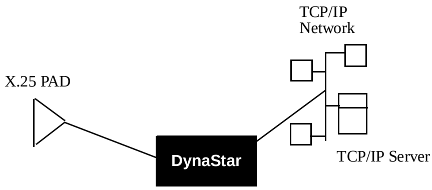


Figure 13-12 X25-In Application

X25-OUT. Figure 13-13 illustrates a typical use of the X25-Out application. In the example, theTelnet client places a call to the IP address assigned to the *DYNASTAR* connection. The *DYNASTAR* checks the IP address in the Telnet request against Async Service entries. If a match is found for an X25-Out configuration, the *DYNASTAR* launches an X.25 call to the X.25 host, based on the X.121 address entered on the same Async Services menu. The X.25 call is processed by the local X.25 routing table before it is passed to the appropriate X.25 port.

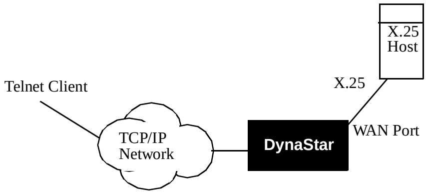


Figure 13-13 Typical X25-Out Application

At this point, the Telnet session is established and the Telnet client is connected to the X.25 host. The session can be cleared by the X.25 device or the Telnet client.

NOTE: X.25 Q, D, and M bits cannot be transported over Telnet and will be lost.

NOTE: X25-Out forwards data to the X.25 host based on TCP packets received and maintains packet boundaries from TCP to X.25. Normal X.3 forwarding conditions defined by Virtual Port 10, X.3 Profile Par 3, 4, and FWD characters are ignored. The only exception is if the TCP packet received is bigger than the X.25 packet size, in which case the TCP packet will be split into two or more X.25 packets.

X25-OUT STREAM. X25-Out Stream service, also available on the Async Services menu, operates like X25-Out, except that it handles data forwarding differently. The X25-Out Stream service forwards data only on the forwarding condition specified by X.3 parameter 3, 4, and the FWD character that is defined in Virtual Port 10 or in the Service X.3 Profile.

X25-OUT-LCN0. The X25-Out-LCN0 service is available to allow monitoring of older devices that perform the X.25 link level but not the packet level. For X25-Out-LCN0 a Telnet session must be opened to the X25 service. The address in this service must route to the port through the X.121 routing table. The call is then accepted internally. Data is received on the physical port on LCN 0 without a restart exchange and with no call setup phase.

MULTICAST. The Multicast service provides a TCP/IP broadcast feature. You can define a maximum of 16 TCP sources that can each connect to up to 16 TCP destinations. For more information on Multicast, see Chapter 12, *The IP/IPX Router Application*.

■ Configuring the Async Services Menu

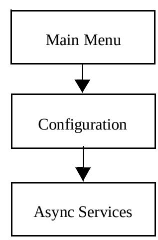
To configure the Async Services menu, follow the procedure below. For information on screen parameters and how they apply to the various service types, see Table 13-2.

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. Select **Async Services**.

✓ The Access Server Commands menu (Figure 13-14) is displayed.

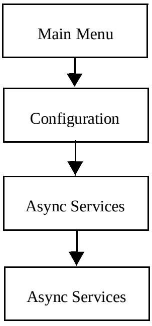



```
                 *** Access Server Commands ***

            1 - PAD configuration options
            2 - PAD profiles
            3 - X.25 Mnemonics
            4 - NUIs
            5 - Async services (PAD, Telnet, IPX-In, SLIP)
            6 - Logoff Scripts
            7 - EPOR Profiles
            8 - Logon Screen  (Initial user screen)
            9 - Multicast Configuration

                 Enter command number:

_________[DynaStar_3df2]__________
Terminate input with <RET>.            Press ESC to return to previous menu.
```

Figure 13-14 Access Server Commands Menu

3. Select **Async Services** again.

✓ The Async Service Names menu (Figure 13-15) is displayed. If no previous entries have been made, the screen is blank. If services have been configured previously, their names are listed on the screen, along with



a number. The screen lists up to 256 entries, which can be viewed by scrolling.

```
                       *** Async Service Names ***
                                    Last changed: 6-6-02 8:26:38

1-Dallas
2-Chicago
3-Reading
4-Columbus
5-Great Falls
6-Burbank
7-Omaha
8-
9-
10-
11-
12-
13-
14-
15-
16-
                         Enter service number:

 _________[DynaStar_3df2]__________
 To add entry, just press <RET>.          Press ESC to return to previous menu.
 To edit entry, enter service # <RET>.    Cursor up/down for more entries
 To delete entry, enter service # <CNTL-D>. Note: delete takes place immediately.
```

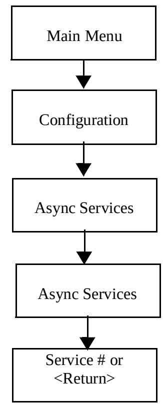
Figure 13-15 Async Service Names Menu

4. To view a new service configuration screen, press **<return>**
OR
To view the screen for an already configured service, type the associated number in the **Enter service number** field and press **<return>**.

✓ A screen similar to Figure 13-16 is displayed. Figure 13-16 shows a default screen that has not yet been configured. If you entered a service number, the settings on the screen reflect the current configuration for that service.

```
                         *** Async Services ***

          Service name:                                        (15)
          Service type:           TELNET
          IP Address              0.0.0.0
          Socket Number:          23
          X.121 address:                                  (15 BCD)
          X.3 Profile:            87 (12) TELNET          (Name or #)
          Telnet command:                                      (23)
          CUG:                                               (0-99)
          Call UserData:                                       (32)
          TCP Idle Timer:         0                (1-255 min., 0=OFF)




_________[DynaStar_3df2]__________           Process selections (Y/N): Y
Use <CTRL-D> to delete entry.           <RET> to toggle or type value
Use TAB & CURSOR keys to move fields.   Press ESC to return to previous menu
```

Figure 13-16 The Async Services Menu (Default Settings)



5. In the **Service name** field, enter a name that will help you identify the configuration. (This name will appear on the Async Services Name menu when you process your selections.)
6. Toggle to select the **Service type**.
7. Make other entries as required.
8. To record your entries, enter **Y** in the **Process selections** field and press **<return>**.

Table 13-2 Async Services Parameters

Parameter	Meaning	Value
Service Name	User entry. Choose a name to help you identify this configuration. Once the name is saved, it can be selected by number on the Async Services Names menu to display your configuration.	Default = Null 15 characters
Service Type	Determines type of async service and use of parameters on the screen. See *Async Service Types* earlier in this chapter for a description of each type.	Telnet (default), IPX-In, SLIP, X25-In, X25-Out, X25-Out Stream, X25-Out-LCN0, Echo Test, Multi-cast
IP Address and Socket Number	**Inbound Services** For Telnet and X25-In, a connection is launched to this IP address and socket when the X.121 address (and CUG, if present) on this menu are called. IP Address and Socket parameters do not apply to IPX-In and SLIP services. **Outbound Services** For X25-Out, X25-Out-LCN0, and X25-Out Stream calls, the *DYNASTAR* checks this IP address and socket against the called address. If there is a match, the *DYNASTAR* places a call to the X.121 address specified on this menu. NOTE: The CUG is not included in outbound calls. **Caution:** Do not use the IP address of the Ethernet Port with the default socket (23), as this will lock you out of the Console port. Avoid using Socket 1998, which is reserved for the XOT function. For information on XOT, see Chapter 6, *The X.25 Application*.	Default for IP address = 0.0.0.0 Any valid IP address (and any socket) on the same network as the Ethernet port (Port 0) can be entered, or the IP address of any other configured WAN port. On a configured WAN port, any socket except 23 can be used. Default for Socket = 23 (Tel-net) Valid entries = 1-65535

Table 13-2 Async Services Parameters (cont.)

Parameter	Meaning	Value
X.121 Address	**Inbound services** For inbound Telnet, X.25-In, SLIP, and IPX-In calls, this address is compared to the X.121 address of incoming X.25 calls. For Telnet and X.25-In, if there is a match, a Telnet session is established using the IP address and socket specified on this menu. For SLIP and IPX-In, if there is a match, the call is passed to the *DYNASTAR*'s regular routing functions. SLIP calls are passed to the IP router; IPX-In calls are passed to the IPX router. (See Chapter 12, *The IP/IPX Router Function*, for more information.) **Outbound services** For X25-Out, X25-Out-LCN0, and X25-Out Stream, a call is launched to the X.121 address if a Telnet connection is made to the IP address and socket specified on this menu.	Default = Null 15 characters

Table 13-2 Async Services Parameters (cont.)

Parameter	Meaning	Value
X.3 Profile	For Telnet or X.25-In, sends a Q packet containing an X.29 Set command, which overwrites X.3 parameters of the calling PAD. For X.25-Out, configures the X.3 parameters of the local virtual X.25-Out service. If the X.3 profile is disabled using CTRL-D to delete the contents of the field, the standard Virtual Port 10 profile is used. Besides whatever profile is assigned, the additional forward condition defined in Virtual Port 10 “forwarding character” is also active. To disable the special forwarding character, use CNTRL-D to delete the contents of the field. Valid forwarding characters are 00 through 7F. The X.3 Profile parameter does not apply to SLIP or IPX-In calls.	Default = 87 (Telnet) Name or number of any profile defined on the X.3 profiles screen. For information on PAD profiles, see Appendix D, *X.3 Profiles and Parameter Settings*.

Table 13-2 Async Services Parameters (cont.)

Parameter	Meaning	Value
Telnet command	**Inbound Services** For Telnet and X25-In, all Telnet commands listed in Table 13-1 that are applicable to a client can be used in establishing a Telnet session. NOTE: For optimum performance, *DYNASTAR* recommends that you enter **-D 8 -Q -N** These parameters set 8-bit data mode, automatically disconnect Telnet when an X.25 Clear is received (or automatically disconnect X.25 if a Telnet clear is received), and inhibit escape to Telnet command mode. Telnet commands do not apply to SLIP or IPX-In calls. **Outbound Services** For X25-Out, X25-Out-LCN0 X25-Out Stream, only the following commands can be used: -H *nnnn* (Sends two bytes as Telnet command) -J (default 8 bit, no negotiation) -LF (strips 'LF' linefeed characters) -N (disables escape) -R (raw mode) -T *type* (defines terminal type)	Default = Null 23 characters Note: Multiple commands can be entered in this field. Separate commands with spaces. For more information, see the section *Telnet Commands* earlier in this chapter.

Table 13-2 Async Services Parameters (cont.)

Parameter	Meaning	Value
CUG (Closed User Group)	A security mechanism that allows only members of the same CUG to communicate with each other. For X25-In and Telnet, the CUG, if entered, is checked along with the X.121 address and must be present in the call request for the call to be accepted. For information on how the various service types are routed, see the previous description of the X.121 Address Parameter. The CUG parameter does not apply to X.25-Out or X25-Out Stream services.	Default = Null Values = 0-99
Call User Data	X25-OUT services can automatically insert a call user data string of up to four characters into the CALL REQUEST packet generated by the *DynaStar*. If no user data is entered, the standard PAD PID is inserted (01000000).	Data string of up to 4 characters
TCP Idle Timer	If the TCP connection has been idle for the configured period of time, a keep alive message is sent. If the server does not receive a response, the message is retried every 45 seconds for 5 times before the session is taken down.	1-255 minutes 0 = off (default)

SNA OVER X.25 AND FRAME RELAY

INTRODUCTION

The DLC-XPAD support available on the *DYNASTAR* allows remote SDLC control units (CUs) to access IBM host computers over public or private X.25 packet data networks (PDNs) as in Figure 14-1. DLC-FRAD support allows the same access over public or private frame relay networks (Figure 14-2). The DLC-FRAD leverages IBM support of frame relay in the NCP and AS/400 platforms.

Unlike traditional bridges and routers, the DLC-XPAD and DLC-FRAD encapsulate SNA LLC2 packets directly inside X.25 packets or frame relay frames, eliminating inefficient SDLC encapsulation over X.25 orIP.

By providing a bidirectional full conversion between SDLC and LLC2, the DLC-XPAD and DLC-FRAD eliminate the substantial overhead, cost, and response time of passing SDLC polls and responses across X.25 or frame relay networks. In conjunction with downstream DLC-XPADs, host-located DLC-XPADs provide the required end-to-end conversion and encapsulation services to and from IBM SDLC hosts. As shown in Figure 14-2, one or more DLC-FRADs located at the host can provide the required conversion and encapsulation services in support of remote DLC-FRADs for users of non-frame relay host computers.

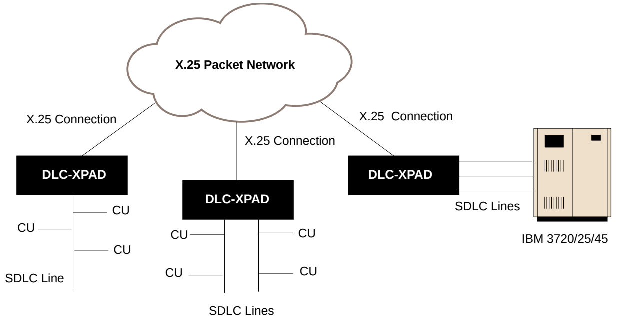


Figure 14-1 Remote Access to an IBM Host via an X.25 Packet Data Network

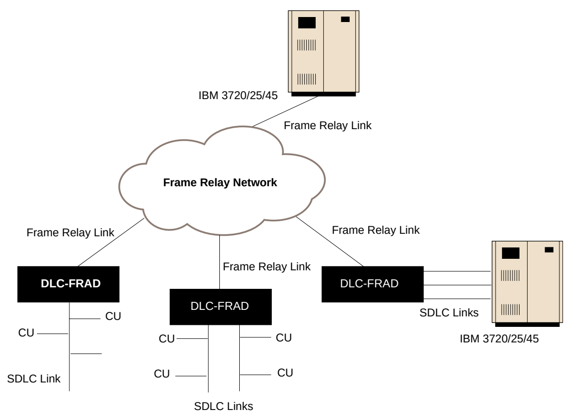


Figure 14-2 Remote Access to IBM Hosts via Frame Relay

LLC Protocol Support

In traditional SNA leased-line environments, the SDLC protocol provides sequencing, error checking, and flow control between adjacent SNA nodes. LLC was developed to provide the same level of service to SNA within a LAN environment. Thus, LLC headers surround the SNA user data over LANs.

An LLC header identifies the session partners via a pair of Service Access Point (SAP) addresses. By carrying LLC as the data portion of an X.25 packet or frame, the X.25 or frame relay network appears to the DLC-XPAD or DLC-FRAD as a virtual LAN.

SDLC control units access that virtual LAN via the DLC-XPAD or DLC-FRAD built-in SDLC-to-LLC conversion services, giving each the appearance of a LAN-attached CU.To let each CU use the LLC services, the DLC-XPAD or DLC-FRAD adopts a scheme in which each CU is represented over the network by a Proxy LAN Physical Unit (PLPU). This allows each CU to indirectly initiate LLC sessions, generate LLC traffic, and be identified as an LLC Service Access Point (SAP) rather than be identified by its SDLC address. Similarly, at the SDLC host site where the DLC-XPAD or DLC-FRAD provides conversion to the host, each CU defined on an SDLC port attached to the host is represented by a PLPU.

The scheme is based on defining a virtual connection between a CU and a PLPU to bind them together at startup.

- For X.25, when an SDLC connection is established with a downstream CU, the PLPU originates the LLC session with a host PLPU defined in the host DLC-XPAD. Each session is conducted over an X.25 virtual circuit established with the host DLC-XPAD.
- For frame relay, when the SDLC connection is established with a downstream CU, the PLPU defined in a DLC-FRAD originates the LLC session with a host PLPU in the host DLC-FRAD or with a specific application residing at the frame relay host. One or more sessions are conducted over a virtual circuit, identified by its Data Link Connection Identifier (DLCI), which interconnects two DLC-FRADs or a DLC-FRAD and an IBM frame relay host.

ENCAPSULATION OF SNA

The DLC-FRAD method of encapsulating LLC2 over frame relay is commonly known as RFC 1490 encapsulation or

direct SNA. This method is the only method that allows encapsulated traffic from remote control units to terminate onto a frame relay NCP without intervening host-located bridges or routers.

Direct SNA, in contrast with bridged SNA, only forwards LLC2 information. It uses a shorter frame by not including the MAC addresses of the session partners and does not use broadcasting to discover the destination address. Instead, the DLC-FRAD uses the LLC2 protocol Service Access Points (SAPs) to identify the session partners. Each SNA session in the DLC-FRAD is uniquely identified by the frame relay DLCI of its PVC route and its SAP addresses carried in the RFC 1490 frames.

The DLC-XPAD borrows its encapsulation technique from frame relay to transport LLC protocol data units (LPDUs) in X.25 packets. To operate over X.25 PDNs that may have packet size restrictions, the DLC-XPAD supports the fragmentation and recombination of LPDUs, allowing X.25 packets as small as 128 bytes. When transmitting an LPDU in multiple X.25 packets, the LLC header information is forwarded only once to reduce overhead.

The DLC-XPAD also improves upon the RFC 1490 methodology by not including the RFC 1490 header in every data packet, relying instead on the X.25 call process to indicate to its session partner the type of encapsulation used for SNA traffic.

SDLC-TO-LLC CONVERSION

Both the DLC-XPAD and the DLC-FRAD terminate SDLC, the link level of SNA, at the entry point(s) of the X.25 or frame relay network. At the terminal site, they are configured to provide a primary SDLC emulation to serially connected SDLC control units, locally terminating the SDLC connections. For X.25, the SDLC traffic is transformed into LLC, encapsulated with an X.25 packet header, and forwarded over the X.25 network. For frame relay, the SDLC traffic is transformed into LLC, encapsulated with both an RFC 1490 header and a Q.922 header, and forwarded over

the frame relay network. Inbound traffic is handled in a reverse manner.

At the host site, the DLC-XPAD or DLC-FRAD is configured to provide a secondary SDLC emulation to the SDLC host, locally terminating the SDLC connections. Through the conversion services provided by the DLC-XPAD or DLC-FRAD, VTAM and NCP view the downstream control units as stations on a private wire multi-point SDLC link. Outbound data from the host is addressed to the control units using SDLC station addresses. The host DLC-XPAD or DLC-FRAD intercepts the SDLC data, converts it to LLC, and encapsulates it as previously described. Inbound traffic is handled in reverse to extract SNA data for forwarding over the SDLC link.

By implementing independent host and terminal SDLC sessions, SDLC polls and acknowledgments do not traverse the network, reducing WAN traffic, packet charges, and possible time-outs.

LLC Sessions over X.25 Virtual Circuits

An LLC session is used to transfer traffic between a downstream PLPU (located at the terminal site) and a host PLPU defined at a host DLC-XPAD. Each session requires an X.25 virtual circuit (VC) to forward traffic over the X.25 PDN.

Thus, each DLC-XPAD's X.25 network interface port used for SNA traffic must support as many X.25 VCs as there are downstream SDLC control units. DLC-XPADs located at the host site must support as many X.25 VCs as necessary to support the aggregate number of simultaneous SNA sessions originating from all downstream DLC-XPADs.

Address Mapping over X.25 Networks

Because DLC-XPADs terminate and route many types of X.25 traffic, they must segregate the inbound X.25 calls carrying LLC traffic. When establishing a switched virtual

circuit (SVC) for forwarding LLC protocol data units, DLC-XPADs signal one another by encoding X.25 Call Request packets with a mutually agreed upon protocol ID (PID). The PID occupies the first 4 bytes of the 16-byte Call User Data (CUD) field of the Call Request Packet. The first byte contains the actual end-to-end protocol identifier followed by two bytes of information for identifying the LLC session partners. The fourth byte is reserved for future use.

By default, the DLC-XPAD sets the PID to 0xC8 to signal that the X.25 payload contains LLC traffic. The PID is followed by the pair of SAP coordinates of the originating PLPU device. Conversely, when a DLC-XPAD receives a call with a PID equal to 0xC8, it examines the next two bytes of that field to determine to which PLPU it should route the call.

The network administrator defines where a DLC-XPAD forwards its SNA traffic by assigning to each PLPU three address coordinates. The first is the X.25 destination address of the destination DLC-XPAD where the partner PLPU resides; the second is a Destination Service Access Point (DSAP) that identifies the partner PLPU; the third is a Source Service Access Point (SSAP) that is used for pairing the incoming call with the local PLPU and for use as a return address for SNA traffic.

PAIRING TERMINAL AND HOST PLPUS. Typically, several downstream DLC-XPADs are configured to forward their SNA traffic to one or more host-located DLC-XPADs (see Figure 14-3).

When aggregating networkwide SNA traffic onto one host DLC-XPAD, all originating PLPUs are assigned the same X.121 destination address, causing their X.25 VCs to terminate onto that DLC-XPAD. To ensure that each calling PLPU maps onto a specific host-configured PLPU, each PLPU is assigned a unique pair of DSAP and SSAP coordinates. The receiving DLC-XPAD uses both pairs of coordinates to bind the calling PLPU to one of its PLPUs.

When aggregating networkwide SNA traffic onto multiple host DLC-XPADs, downstream PLPUs terminating in different host DLC-XPADs have different X.121 addresses but can have the same DSAP value.

Recipient PLPUs must also be configured with the X.121 address of the DLC-XPAD where their calling PLPU partner resides. This enables the bandwidth-on-demand feature described in the section *X.25 Call Establishment and Clearing*.

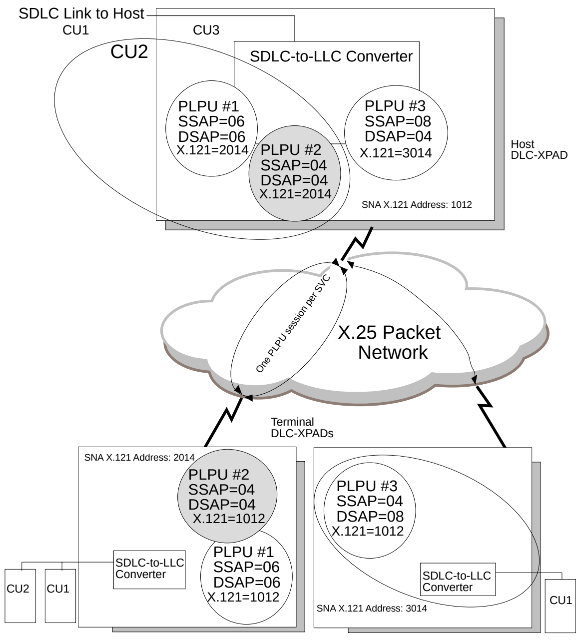


Figure 14-3 CU-to-CU Address Mapping over X.25 Packet Data Networks

ADDRESS MAPPING OVER FRAME RELAY

There is no dynamic procedure to identify the use of RFC 1490 on a given DLCI. The DLC-FRAD at both ends of a frame relay network must have prior knowledge of the virtual circuits on which RFC 1490 encapsulation is employed and must be configured accordingly. The DLC-FRAD allows the user to define on which virtual circuits direct SNA traffic is routed. Each PLPU is assigned a DLCI over which to forward its LLC traffic.

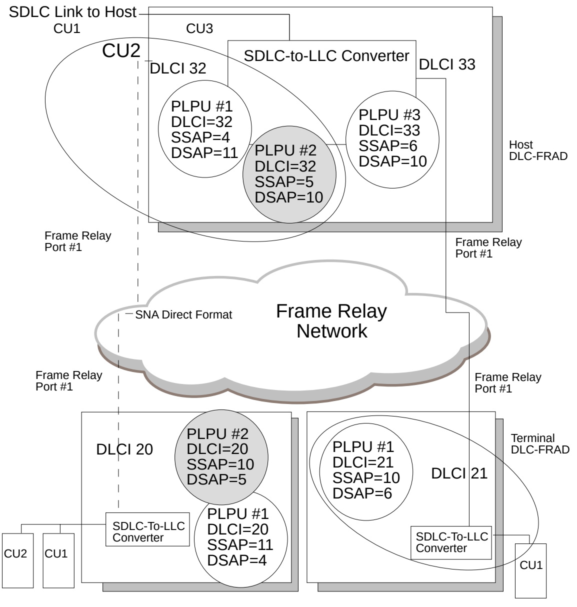


Figure 14-4 CU Address Mapping over Frame Relay

To interoperate with other LLC SAPs (for example, SNA at the host), a PLPU is assigned both a source and a destination Service Access Point, referred to as SSAP and DSAP. The SSAP identifies the PLPU; the DSAP identifies its target partner. Traffic routing over the network assumes that each DLCI is appropriately bound by the network provider to another DLCI of the target DLC-FRAD or the NCP as illustrated in Figure 14-4.

A DLC-FRAD examines incoming RFC 1490 traffic over each of its DLCIs configured for direct SNA. The targeted PLPU is identified by the value of the DSAP field of each incoming frame. In turn, the PLPU traffic is converted and forwarded to the local CU associated with that PLPU.

MULTIPLEXING LLC2 SESSIONS OVER A DLCI.

The DLC-FRAD can multiplex several LLC sessions over a single frame relay PVC. Each LLC session transfers traffic between a PLPU and a remote SAP or another PLPU. The DLC-FRAD demultiplexes the LLC traffic, based on the

DSAP in the LLC header, and sends it to its appropriate PLPU destination.

ATTACHING TO AN IBM HOST. When SNA traffic is terminated directly onto an IBM frame relay host, each PLPU session on the network is uniquely identified by a combination of its source Service Access Point (SSAP) and the DLCI it is assigned. As each DLCI can carry several LLC sessions, the SSAP uniquely identifies the PLPU. All PLPUs would be assigned the same destination SAP to cause their traffic to be forwarded to the SNA application.

PAIRING TERMINAL AND HOST DLC-FRADS. To bind a DLC-FRAD's downstream PLPU with an upstream PLPU, the downstream PLPU is assigned a DSAP equivalent to the SSAP of the upstream PLPU. The combination of DLCI and DSAP values provides a unique identifier for the receiving DLC-FRAD to map an incoming connection to one of its PLPUs.

X.25 CALL ESTABLISHMENT AND CLEARING

LLC sessions over an X.25 network are initiated by DLC-XPADs attached to SDLC control units. When a DLC-XPAD establishes the synchronous data link level with a downstream CU, it places an X.25 call. If the destination DLC-XPAD accepts the call, it in turn establishes the synchronous data link connection with the host on behalf of the calling CU, allowing the host to activate the SNA session and the exchange of end-to-end traffic.

Where it is not practical to maintain an SVC for each CU that is powered on, the network administrator may elect to define an X.25 inactivity timer to disconnect idle SVCs. The DLC-XPAD supports a dynamic bandwidth-on-demand feature by maintaining the LLC session when the underlying X.25 SVC is cleared because of the inactivity timer or because of a momentary failure of the X.25 network. This feature preserves the integrity of the SNA session, avoiding accidental clearing of SNA sessions when the host response time or the user's think-time triggers the inactivity timer.

Since either end can reestablish the SVC to forward data from attached SDLC equipment, PLPUs at both ends of the network must be configured with the DLC-XPAD X.121 address of their respective PLPU partners.

■ CONFIGURATION OVERVIEW

Configuration of the DLC-XPAD or DLC-FRAD consists of three main steps, some of which have substeps. The order to follow when you configure the DLC-XPAD or DLC-FRAD is given below. The differences in configuring a DLC-XPAD or a DLC-FRAD are noted.

1. Configure the SDLC access ports.

2. Configure the X.25/frame relay parameters.

- Configure the network ports.
- Set up the routing table (DLC-XPAD only).
- Configure DLCIs (DLC-FRAD only).

3. Configure the SDLC/SNA parameters.

- Define the SDLC Control Units.
- Configure the LLC attributes of each Proxy LAN PU (PLPU).
- Map each CU to a PLPU.
- Set SNA X.25 SVC parameters (DLC-XPAD only).

If you make a mistake while configuring your SDLC connections, an error message appears on the screen. Error messages are explained in Table 14-6 at the end of the chapter.

CONFIGURE SDLC ACCESS PORTS

Operation of the DLC-XPAD or DLC-FRAD requires that you define one or more SDLC ports. If you edit the configuration of an SDLC port while SNA service is in progress, the current sessions are terminated. To restart the service, see the later section *Enabling SNAParameters*.

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. Select **Port**.

✓ A list of available ports is displayed.

3. Select a port that will use the SDLC protocol.

✓ The configuration screen for the selected port is displayed.

4. Toggle to select **SDLC Term** if you wish to configure a port that will attach SDLC controllers.
   OR
   Select **SDLC Host** if you wish to configure a port that will attach SDLC host computers.

   NOTE: To delete or reassign an SDLC port, first delete/reassign all the SDLC control units configured for that port.

✓ If you select **SDLC Term**, a screen similar to the one in Figure 14-5 is displayed. If you select **SDLC Host**, a screen similar to the one in Figure 14-6 is displayed. The information on these screens is explained in Table 14-1.

5. Configure the screen parameters as appropriate for your network. Refer to Table 14-1 for parameter values and explanations.

6. When your entries are complete, enter **Y** in the **Accept changes** field and press **<return>**.

✓ You return to the Configure Port screen. The message *Changes made for Port n* appears near the bottom of the screen. The message *Config has changed: use CTRL-W to save* also appears. These changes are not yet activated, even if you use the CTRL-W command.

7. Continue your configuration as explained in the next section, *Configure the X.25/Frame Relay Parameters*.

   NOTE: Before activating SDLC/SNA changes, see the section *Enabling Parameters* later in this chapter.

Once an SDLC port has been created and edited, the **SNA** selection in the Configuration Commands screen is followed by an asterisk. The asterisk is displayed until you activate the changes by making the appropriate selection from the SNA Configuration screen (selection 9) or by resetting the *DYNASTAR*.

```
                   ***SDLC Terminal Port Configuration***
Port: 101   IS-232                                 Last changed: 6-6-02 11:33:33

  |- Press <RET> to toggle values -||– Type in values.  Max chars shown in () --|
  Port type:   SDLC Term             Port name:      Term Port                 (14)

  Connection mode:        DIRECT
  Connection type:        PT-TO-PT

  Line speed:             9.6 kbps
  SDLC extended:          N
  NRZ/NRZI:               NRZI
  __________________________ Type in values _______________________
  T1 Acknowledgement timer:  1  (secs)      Tx Window size:      1
                                             N2 Retry count:      10  (retries)
  Slow Poll timer:               1


_______[DynaStar  dc000345]_______                    Accept changes (Y/N): Y
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 14-5   SDLC Terminal Port Configuration Screen

```
                   ***SDLC Host Port Configuration***
Port: 101   IS-232                                 Last changed: 6-6-02 11:22:33

  |- Press <RET> to toggle values -||-- Type in values.  Max chars shown in () --|
  Port type:   SDLC Host            Port name:      Host  A port          (14)

  Connection mode:     DIRECT
  Connection type:     MULTI-PT

  Line speed:          9.6 kbps
  SDLC extended:       N
  NRZ/NRZI:            NRZI



_______[DynaStar  dc000345]_______                    Accept changes (Y/N): Y
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 14-6   SDLC Host Port Configuration Screen

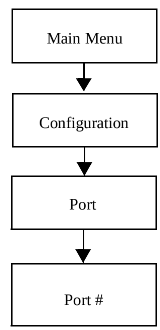


Table 14-1 SDLC Port Parameter s

Parameter	Description	Values
Port name	A name to help identify this port.	Max 14 chars
Connection mode	Determines whether this port appears as a DTE or a DCE. DIRECT makes the port appear as a DCE; LEASED makes the port appear as a DTE. For ports defined as SDLC Term, the Connection Mode can also be set to Dial to support dial-in connections.	Leased Direct (default) Dial
Connection type	Determines multipoint or point-to-point configuration. For ports defined as Dial, only the point-to-point connection type is allowed. If set to Pt-to-Pt and Dial, the SDLC Term ports poll using 0xFF.	Pt-to-Pt (default for SDLC Term) Multi-PT (default for SDLC Host)
Line speed	If Connection mode is set to Direct, the port uses this parameter to set its output transmit clock.	9.6 (default), 19.2, 38.4, 56, 64, 128, 256, 512, 1024, 1544, 2048 kbps
SDLC extended	Determines Modulo 8 or 128.	N=8 (default) Y=128
NRZ/NRZI	Determines the coding of SDLC transmission.	NRZ NRZI (default)
T1 Acknowl-edgment timer	Determines the no-response time-out. When the timer expires, transmission is retried until the N2 Retry counter expires.	1-255 sec 1=default
TX Window size	Determines the maximum window size that the DLC-XPAD or DLC-FRAD will use with this control unit.	1-128 1=default
N2 Retry count	Number of retry attempts after a no-response time-out. The device is then placed in the slow poll timer mode, and its LLC session is terminated. Polling resumes with an XID poll at a frequency defined by the slow poll timer.	1-20 10=default

Table 14-1 SDLC Port Parameters (cont.)

Parameter	Description	Values
Slow Poll timer	Determines the frequency of polling in the slow poll timer mode.	1-255 sec 1=default

CONFIGURE THE X.25/FRAME RELAY PARAMETERS

The second step in the configuration of the DLC-XPAD or DLC-FRAD is to configure the X.25 or frame relay parameters. This is divided into two steps—configuring the network ports and configuring the routing parameters (DLC-XPAD) or DLCIs (DLC-FRAD)—and must be done before you configure the SNA parameters.

CONFIGURE PORTS. You must define one or more network ports before the DLC-XPAD or DLC-FRAD can be enabled.

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. Select **Port**.

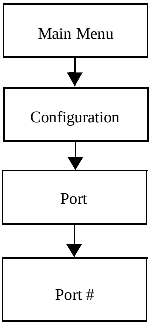
✓ A list of available ports is displayed.

3. Select a port that will use the X.25 protocol.
OR
Select a port that will use frame relay protocol.

✓ A screen similar to the one shown in Figure 14-7 or Figure 14-8 is displayed.

```
                     ***X.25 Port Configuration***
Port: 5  IS-35                                 Last changed:  6-6-02  11:26:45

|- Press <RET> to toggle values. -|  |-Type in values. Max chars shown in () --|
Port type:            X.25 line          Port name:   HS WAN 1                 (14)
                                          X.121 Address:                  (15 BCD)
Connection mode:              DTE
Line speed:               9.6 kbps        Non-Zero DTE Cause:    N
Number of flags:(0-15)           0        Allow User Data:       Y
Calling address mod:          NONE        LAPB extended:         N
Local Address insert:            N        X.25 mode:             DTE
Max Window size:                 7        K LAPB window size:    7             (fixed)
Max Packet size:              1024        T1 Acknowledgment timer:3        (1-255 sec)
Packet/Window Neg:               Y        T3 Idle Timer:         30        (0-255 sec)
Require CUG:                     N        N2 Retransmission count:20           (1-255)
Require NUI:                     N        N1 Max frame size:     8248 bits
Req Reverse Charging:            N        LCN Partition    Base LCN     Number of VCs
Route inbound calls on CUD:   N                            (1-4095)
Traffic types permitted on line             Permanent:      1               0
     IP Routing:                 Y          One-way in:     1               0
     IPX Routing:                Y          Two-way:        1               4095
     Ethernet Bridging:          Y          One-way out:    4095            0

_______[DynaStar_3614]_______                  Process selections (Y/N): Y
Use TAB & CURSOR keys to move among fields.   Press ESC to abort command & exit.
```

Figure 14-7   X.25 Port Configuration Screen




```
                  ***Frame Relay Port Configuration***
Port: 5   IS-35                                Last changed:  6-6-02  11:26:45


 |- Press <RET> to toggle values -||–Type in values.  Max chars shown in () --|
 Port type:   frame relay            Port name:      FRelay SNA           (14)

 Connection mode:    DTE

 Line speed:         56.0 kbps
 DLCI management:    LMI                       User, Network, or NNI: USER
 Circuit backup:     N

Traffic types permitted on line
   IP Routing:                 Y
   IPX Routing:                N
   Ethernet Bridging:          N

UNI/NNI Fragmentation: None



________[DynaStar_3614]_________               Process selections (Y/N): Y
Use TAB & CURSOR keys to move among fields.   Press ESC to abort command & exit.
```

Figure 14-8   Frame Relay Port Configuration Screen

4. Configure the screen parameters as required for your network. (See Chapter 6, *The X.25 Application*, if you are configuring an X.25 port. See Chapter 8, *The Frame Relay Application*, if you are configuring a frame relay port.)

5. When your entries are complete, enter **Y** in the **Process selections** field and press **<return>**.

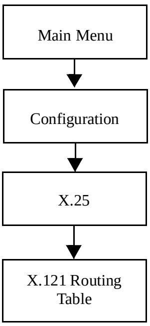
✓ You return to the Configure Port screen.

6. If you are configuring an X.25 connection, continue with the configuration as described in the next section, *Configure the Routing Table.*
   OR
   If you are configuring a frame relay connection, skip to the section *Configure DLCIs.*

CONFIGURE THE ROUTING TABLE (DLC-XPAD ONLY). The X.25 Routing table is used to route calls from the unit's SNA module to outbound X.25 lines. It is not used to route incoming calls from the X.25 network.

Configure the X.121 address (using an explicit address or an address with wildcards) for each remote DLC-XPAD that terminates SNA session(s) across the network. This address must match the one configured for the remote XPAD (Figure 14-17). This will allow X.25 calls made from the local PLPU(s) to reach the PLPU session partner(s) in the remote DLC-XPAD(s).

You define the addresses in the screen shown in Figure 14-9. Please refer to Chapter 6, *The X.25 Application*, for further details on how to configure this screen.




```
                   ***X.25 Concentrator Routing Table***
                                         Last changed: 4-23-02  7:00:45

  X.121 address    Shared   |-------Use RET to Toggle -----|   X.32 dial line phone #
 (1-15 BCD, D&X) Scheme    Port     Priority   Dial Speed       (max 19 characters)
1:
2:
3:
4:
5:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:
_______[DynaStar 35dd]_______                         Process Routing tables (Y/N):
Search for X.121 address:                             Select Share Scheme:
To change or add entry, enter new value.              Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among entries. Press ESC to abort command & exit.
```

Figure 14-9 X.25 Concentrator Routing Table

CONFIGURE DLCIS (DLC-FRAD ONLY). For each frame relay port, network assigned DLCIs must be configured. Any of the defined DLCIs can later be assigned to transport one or more direct SNA sessions. This SNA traffic can be multiplexed with non-SNA traffic; however, be careful that this does not adversely affect SNA performance. To dedicate a DLCI to SNA traffic, do ***not*** enable Bridged, IPX, or IP traffic.

To configure DLCIs:

1. From the Main menu, select **Configuration**.

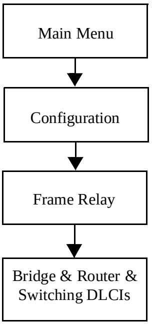
✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. Select **Frame Relay**.

✓ The Frame Relay Parameters menu (Figure 8-3) is displayed.

3. Select **Bridge, Router & Switching DLCIs**.

✓ The screen shown in Figure 14-10 is displayed.




```
             ***Frame Relay Switching, Routing, Bridging, and SNA Table***
                                                   Last changed:  4-23-02  11:26:45

             Inbound     Outbound                        CIR  Fragmnt
 Type      Port  DLCI  Port   DLCI  B   IPX  IP   PRTY  Kbps   Bytes     Dist IP Address
1: Switching  5    23    101     55                  1    56.0k
2:
3:
4:
5:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:

 ________[DynaStar_3614]_________             Process Table selections (Y/N): Y
In Type field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.                 Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields.    Press ESC to abort command & exit.
```

Figure 14-10 Frame Relay Switching, Routing, Bridging, and SNA Table

4. Configure the DLCIs for the frame relay ports. See Chapter 8, *The Frame Relay Application*, for detailed information on how to complete this screen.

5. When your entries are complete, enter **Y** in the **Process Table selections** field and press **<return>**.

✓ You return to the Frame Relay Parameters menu. Your entries are applied to the next call on the frame relay ports configured.

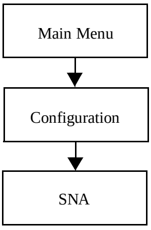
SET SNA PARAMETERS

Once you have defined the SDLC ports and the X.25-related or frame-related parameters, you can define the SNA parameters.

The definition of the SNA parameters is divided into four categories:

- The attributes of the control units
- The profile of each Proxy LAN PU (PLPU)
- The virtual connections that bind CU-SDLC sessions to PLPU-LLC sessions
- (DLC-XPAD only) The underlying X.25 SVC parameters that support the SNA operation

The procedures that follow start from the SNA Configuration menu, shown in Figure 14-11. You access this screen by selecting **Configuration** from the Main menu and then **SNA** from the Configuration Commands menu.



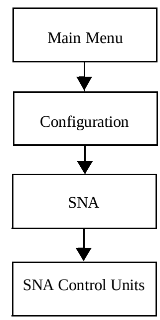

```
                         ***SNA Configuration***


              1 - SNA Control Units
              2 - PLPU Sessions
              3 - PLPU and CU Virtual Connections Map
              4 - SNA X25 SVC Parameters




                      Enter command number:


 ________[DynaStar_3614]_________
Terminate input with <RET>.             Press ESC to return to previous menu.
```

Figure 14-11 SNA Configuration Menu

CONFIGURE SDLC CONTROL UNITS. To configure the SDLC control units:

1. From the SNA Configuration menu (Figure 14-11), select **SNA Control Units**.

✓ A screen similar to the one in Figure 14-12 is displayed.




```
                         ***SNA Control Units***
                                       Last changed:  4-23-02  11:26:45

             Address          |----Use <RET> to toggle values----|
        Name     Cu     Grp  Port   Type
 1:     mycu1   40      00      3    PU 1/5294
 2:     mycu2   41      00      3    PU 2
 3:
 4:
 5:
 6:
 7:
 8:
 9:
10:
11:
12:
13:
14:
15:
16:

________[DynaStar_3505]________                  Accept changes (Y/N): Y
 In NAME field, use UP/DOWN to scroll and LEFT to process selections.
 To change or add entry, enternew value.        Use <CTRL-D> to delete entry.
 UseTAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 14-12 SNA Control Units Screen

2. Complete the fields as required. The fields are explained in Table 14-2.

NOTE: You can configure up to 64 CUs on this screen. In addition to identifying a CU for subsequent association with a PLPU, the unique **Name** assigned to each CU typically reflects its location or the identity of its operator for management purposes. The **Name** is of local significance only. The DLC-XPAD or DLC-FRAD displays the numbers of the port(s) configured for SDLC support. You can toggle through available ports to make your selection.

3. When you have configured all the CUs, enter **Y** in the **Accept changes** field and press **<return>**.

✓ You return to the SNA Configuration menu (Figure 14-11). If you have made changes, an additional option, **Accept all SNA changes-Service will be restarted** appears on the screen.

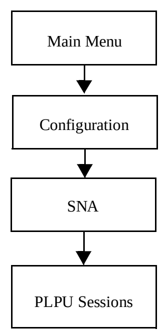
Table 14-2 SNA Control Unit Parameter s

Parameter	Description	Values
Name	Unit internal name used for associating a CU to a PLPU.	8 characters Space and Tab not valid Default=null
CU Address	Determines the address by which the CU is polled.	0x01-0xFE=dedicated connection 0xFF=dial-in connection Default=00 (not active)
Group Address	Only applicable to CUs defined on SDLC Host ports. Determines the group poll address for that PU if the host uses group poll on that port.	0x01-0xFE 0 = Specific poll
Port	*DYNASTAR* port the CU will use. Toggle through available ports.	Any port number pre-configured for SDLC support
Type	Determines the PU type of the attached SDLC CU or of the CU being polled from the SDLC host. The implication of this setting is further described in the section that follows.	PU 1/5294=5294 PU 1/5394=5394 PU 2=3x74, 3270 PC, 3700, 4700 PU 2.1=AS/400, APPC/PC, S/36 Default=PU1

DEFINE PLPU SESSION ATTRIBUTES. When you have finished defining the CUs, you must configure the LLC attributes of each PLPU session carried over the network.

To define the profile for each PLPU session:

1. Select **PLPU Sessions** from the SNA Configuration screen.



✓ A screen summarizing all configured PLPU sessions is displayed (Figure 14-13). The screen displays parameters that are common to the SNA over X.25 (DLC-XPAD) and SNA over frame relay (DLC-FRAD) environments. If the unit is configured only to forward SNA over X.25, the **DLCI** and **Port** fields, which pertain to frame relay, will be blank.

```
                         ***Summary of PLPU Profiles***
                                              Last changed:  4-23-02  11:26:45
  |_________Display Only Fields__________|
  #  Name      Port   DLCI  DSAP SSAP          X.121 Address
  1:  plpu1                  08      04         311012345678901
  2:  plpu2                  08      06         311012345678901
  3:                         00      00
  4:                         00      00
  5:                         00      00
  6:                         00      00
  7:                         00      00
  8:                         00      00
  9:                         00      00
 10:                         00      00
 11:                         00      00
 12:                         00      00
 13:                         00      00
 14:                         00      00
 15:                         00      00

________[DynaStar_3505]________
 In NAME field, use UP/DOWN to scroll and RET to access PLPU parameters screen.
 Use <CTRL-D> to delete entry.                  Press ESC to return to previous menu.
```

Figure 14-13 Summary of PLPU Profiles Screen

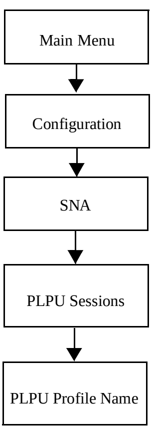
2. Select a value in the **Name** field or select an empty name for a new entry and press **<return>**.

✓ The PLPU Sessions screen, shown in Figure 14-14 (X.25) and Figure 14-15 (frame relay), appears. The new screen prompts you to add a PLPU profile or to change an existing profile.

3. Select **X.25** or **Frame Relay** as the **Network Type**.

4. Configure the remaining LLC parameters as required. Table 14-3 gives parameter meanings and values.

CAUTION: This screen defines the parameters that govern the LLC session of the particular PLPU. Because the DLC-XPAD does not automatically disconnect an LLC session when disconnecting an idle X.25 SVC, you must be careful when selecting the values of the LLC parameters. For example, an LLC inactivity timer (Ti) that is smaller than the X.25 inactivity timer (defined in the SNA X.25 SVC Parameters screen, Figure 14-17) will force the DLC-XPAD to maintain the X.25 SVC for the sole purpose of forwarding LLC “Are you alive” polls.

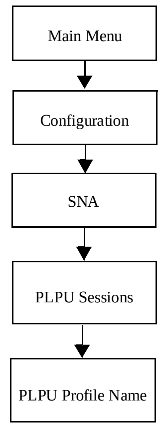



```
                          ***PLPU Sessions***

|_____ Type in values_____|              | Use RET to toggle options |
Name:  plpu1    (8 char max)              Network Type: X.25
SSAP:  04     (2 hex digits)
DSAP:  04     (2 hex digits)

T1:  3   (in secs)    T2: 0    (in secs)   0       0
Ti:  30  (in secs)

N2:  3            N3:   1                    | Enter X.25 values |
Tw:   7           Rw:   7                    X.121 address: 311012345678901

________[DynaStar_3505]________                      Accept changes (Y/N): Y
Use TAB & CURSOR keys to move among fields. Press ESC to return to previous menu.
```

Figure 14-14 PLPU Sessions Screen for X.25

```
***PLPU Sessions***

| Type in values |                              | Use RET to toggle options |
Name: plpu2   (8 char max)                       Network Type: Frame Relay
SSAP: 06    (2 hex digits)
DSAP: 08    (2 hex digits)                     | Use RET to toggle Port values |
                                                 Port  DLCI
                                                  5     16
  T1: 3  (in secs)   T2: 0   (in secs)
  Ti: 30 (in secs)

  N2: 3          N3:  1
  Tw:  7         Rw:  7



________[DynaStar_3505]________                          Accept changes (Y/N): Y
Use TAB & CURSOR keys to move among fields. Press ESC to return to previous menu.
```

Figure 14-15 PLPU Sessions Screen for Frame Relay



5. (DLC-XPAD only) After configuring the LLC parameters, define the X.121 address. This is the address of the remote DLC-XPAD's SNA module where the PLPU partner can be reached. You must have previously defined this address in the X.25 Concentrator Routing table (Figure 14-9).

6. When you have finished configuring this screen, enter **Y** in the **Accept changes** field and press <**return**>.

✓ You return to the Summary of PLPU Profiles screen (Figure 14-13).

7. Repeat steps 2 through 6 for more entries or changes.

8. When all PLPU profiles have been defined, press <**ESC**> from the Summary of PLPU Profiles screen.

✓ You return to the SNA Configuration screen. If you have made changes, the option **Accept all SNA changes-Service will be restarted** appears on the screen.

Table 14-3 PLPU Session Parameters

Parameter	Description	Values
Name	PLPU internal name. Used to pair each PLPU session profile with a control unit to route outgoing and incoming traffic to and from the control units.	8 characters Space and Tab not valid Default=null
Network Type	Identifies the type of network for forwarding the SNA traffic.	Frame Relay X.25
SSAP (Source Service Access Point)	Identity of the local PLPU. Must be unique within a DLC-XPAD/FRAD. Incoming traffic with DSAP and SSAP coordinates equal to the PLPU's SAP coordinates is routed to that PLPU.	0x04-0xFE Default=null
DSAP (Destination Service Access Point)	Identity of the remote PLPU. This must equal the SSAP of the targeted PLPU.	0x04-0xFE Default=null
T1 (LLC reply timer)	Acknowledgment must be received before this timer expires.	0-255 sec. 3=default
T2 (Frame Acknowledgment delay timer)	Started when a frame requiring acknowledgment is received. Used to delay the generation of an LLC RR frame, increasing the chance for piggybacking the acknowledgment with an I-frame. The value of T2 must not be greater than the value of T1.	0-255 sec. 0=default
Ti (Inactivity timer)	Receiver Acknowledgment timer. Must always be greater than T1. This variable will verify that the logical connection is up by polling with an RR (keep-alive packet). The T1 timer is started upon transmission.	0-255 sec. 30=default NOTE: Value must be greater than the value of the SNA X.25 inactivity timer (Table 14-5).

Table 14-3 PLPU Session Parameters (cont.)

N2 (Retry counter)	Number of times to retransmit an unacknowledged I-frame to a network destination before attempting logical link recovery procedures.	1-20 3=default
N3 (Ack Delay counter)	Used with T2 to allow the reduction of acknowledgment traffic by not immediately acknowledging I-LPDUs.	1-20 1=default
Tw	Max Outstanding LPDUs. The maximum number of I-LPDUs outstanding at any given time.	1-128 7=default
Rw	Receive Window Size. The number of I-frames received before acknowledgment.	1-128 7=default
Port	Target frame relay port to carry the session. (Displayed when Frame Relay is selected as Network Type.)	Any port capable of carrying frame relay. Default=null
DLCI	Identifies the Frame Relay data link connection for the PLPU session. The combined values of the DLCI and the DSAP uniquely identify a target PLPU. (Displayed when Frame Relay is selected as Network Type.)	16-1022 Default=null
X.121 address	Network address of the SNA module at the remote DLC-XPAD. (Displayed when X.25 is selected as Network Type.)	1-15 BCD digits Default=null NOTE: Legal addresses are those already defined in the X.121 routing table (under the X.25 Configuration menu).

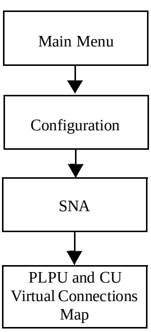
MAP EACH CU TO A PLPU. The third step in the SNA configuration is to map each CU to a PLPU. For a terminal DLC-XPAD or DLC-FRAD, each CU should be configured as a downstream connection, while the LLC or LLC2 session is the upstream connection. The terminal DLC-XPAD or DLC-FRAD establishes the data link with the CU prior to establishing the LLC connection over the network.

For a host DLC-XPAD or DLC-FRAD, each CU polled by the host is configured as an upstream connection, while the LLC session is the downstream connection. Once the downstream LLC connection of a host DLC-XPAD or DLC-FRAD is up with a remote DLC-XPAD or DLC-FRAD, the host DLC-XPAD or DLC-FRAD activates the data transfer mode for each PU being polled by the SDLC host and for which a PLPU session is established.

To map a CU to a PLPU:

1. From the SNA Configuration menu, select **PLPU and CU Virtual Connections Map**.

✓ A screen similar to the one in Figure 14-16 is displayed.




```
                    ***PLPU and CU Virtual Connections Map***
                                               Last changed: 3-23-02 13:24:44

        |Use RET to toggle values|
        Downstream        Upstream                 | Type in value for PU2 - optional |
        Type    Name     Type    Name                 XID
1:      SDLC    CU1      LLC     PLPU1
2:
3:
4:
5:
6:
7:
8:
9:
10:
11:
12:
13:
14:
15:
16:
 ________[DynaStar_3505]________                          Accept changes (Y/N): Y
In TYPE field, use UP/DOWN to scroll.
To change or add entry, enter new value.          Use <CTRL-D> to delete entry.
```

Figure 14-16 PLPU and CU Virtual Connections Map

2. Fill in appropriate values. Table 14-4 describes the parameters and their values.

3. Once you have made your entries, enter **Y** in the field **Accept changes** and press **<return>**.

✓ You return to the SNA Configuration screen. If you have made changes, the option **Accept all SNA changes-Service will be restarted** appears on the screen.

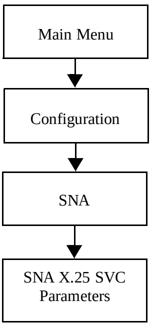
Table 14-4 PLPU-CU Virtual Connection Parameters

Parameter	Description	Values
Downstream Type	Determines if the downstream connection is an SDLC controller or LLC.	LLC or SDLC Default=null
Downstream Name	Name of the device associated with the downstream connection.	CU or PLPU name Default=null
Upstream Type	Determines if the upstream connection is an SDLC host or LLC.	LLC or SDLC Default=null
Upstream Name	Name of the device associated with the upstream connection.	CU or PLPU name Default=null
XID	This variable allows the DLC-XPAD or DLC-FRAD to propagate the XID end-to-end or to generate it locally. When the XID is configured and the CU type associated with this PLPU is type 2, the XID response is formatted and generated locally using the poll address configured for that CU in the PUID field of the XID response. For PU1 and PU2.1, this field must be left blank. For a PU1, the DLC-XPAD or DLC-FRAD generates the XID locally as described above for the PU2. For PU2.1, the user must leave this field blank to allow XID negotiation. The DLC-XPAD or DLC-FRAD does not generate a PU3 XID.	8 hex characters. The DLC-XPAD or DLC-FRAD uses this value to encode both the Block number and the PUID of the PU2 XID response. In addition, it uses the CU Address value to encode the corresponding field in the PU2 XID response.

CONFIGURE SNA X.25 PARAMETERS (DLC-XPAD ONLY). To configure SNA X.25 parameters:

1. From the SNA Configuration menu, select **SNA X.25 SVC Parameters**.

✓ A screen similar to the one in Figure 14-17 is displayed.



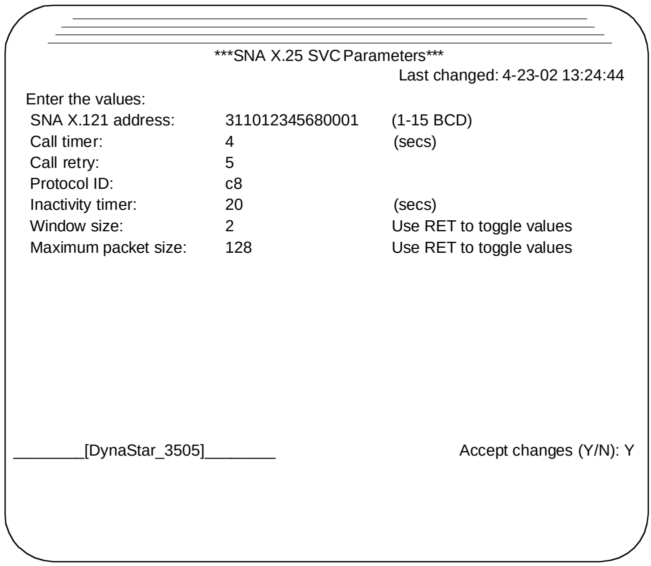


Figure 14-17 SNA X.25 SVC Parameters Screen

2. Fill in appropriate values. Table 14-5 describes the parameters and possible values.

3. Once you have made your entries, enter **Y** in the field **Accept changes** and press **<return>**.

✓ You return to the SNA Configuration screen. If you have made changes, the option **Accept all SNA changes-Service will be restarted** appears.

Table 14-5 SNA X.25 Parameter s

Parameter	Description	Value
SNA X.121 address	Determines the local address of the resident X.25 SNA module. The *DYNASTAR* needs this to route incoming calls to the DLC-XPAD module.	1-15 BCD digits Default=null
Call timer	Response to an X.25 call request is expected within this amount of time.	1-9999 secs 4=default
Call retry	Determines the maximum number of call retries that should be attempted if the response to an X.25 call request is not received within the amount of time defined by the call timer. Once the number of retries is exhausted, the DLC-XPAD waits for another LLC packet to reestablish an X.25 SVC.	1-20 5=default
Protocol ID	Determines the value of the PID, which indicates that the X.25 call carries LLC traffic. Both originating and receiving DLC-XPADs must be configured with the same value.	2 hex chars 00 not allowed C8=default
Inactivity timer	Determines the length of time an X.25 SVC can remain idle before being cleared. This timer should be less than the smallest LLC Ti timer (PLPU session parameters) defined in the unit.	1-9999 secs 20=default
Window size	Determines the maximum number of packets that can be transmitted by the DLC-XPAD over the X.25 network before it receives an acknowledgment.	2-7 2=default
Maximum packet size	Determines the maximum size of the payload field (contains LLC protocol data unit) carried in an X.25 data packet. Larger packet sizes minimize fragmentation.	128 (default), 256, 512, 1024

ENABLE SNA PARAMETERS

Because the SNA parameters are so interdependent, values assigned to the parameters take effect only when you select the option **Accept all SNA changes** from the SNA Configuration screen, which restarts the *DYNASTAR*.

Whenever you have made changes but not activated them, the SNA selection in the Configuration Commands screen will be displayed followed by an asterisk. The asterisk remains until you accept the changes or reset the unit.

To activate SNA changes:

1. To avoid disrupting ongoing SNA activities, disable all SDLC ports. (Access the Disable Port menu from the Status menu. See Chapter 4, *System Functions and Parameters*, for detailed information.)
2. From the Configuration Commands menu, select **SNA**.

✓ The SNA Configuration menu (Figure 14-11) appears.

3. Select the option **Accept all SNA changes-Service will be restarted**.

   NOTE: This option is available only if changes have been made but not activated.

✓ The changes are activated and the SNA service is restarted.

4. Enable all SDLC ports. (Access the Enable Port menu from the Status menu. See Chapter 4, *System Functions and Parameters*, for detailed information.)

■ CONFIGURATOR ERROR MESSAGES

Table 14-6 summarizes the configurator error messages related to the DLC-XPAD or DLC-FRAD implementation. These messages are displayed on the configuration screens during the configuration process. The table includes error messages for both SNA over X.25 and SNA over frame relay.

Table 14-6 Configurator Error Messages

Message	Problem
CU or PLPU Not Configured	You failed to configure CUs or PLPU sessions from the SNA Configuration menu prior to attempting this selection.
DLCI Does Not Exist	The DLCI you assigned to the selected frame relay port is not defined in the DLCIs for SNA, Bridge, and Router Calls screen.
DUP Addr	You configured more than one CU on a port with the same CU address. (CUs with the same PU addresses can be configured only if they belong to different ports.)
DUP CU Names	You configured more than one CU in the unit with the same CU name.
Dup DLCI & SSAP Combination	You have assigned the same combination of DLCI and SSAP values to more than one LLC unit on the same port. Two LLC units cannot have the same combination of DLCI and SSAP if they are configured on the same port.
Invalid CU	You tried to configure more than one CU on a point-to-point link.
Invalid CU Addr	1) Connection type of the port is multipoint and the configured CU address is 0xFF. 2) Connection mode of the port is dial-up and the configured CU address is not 0xFF. 3) PU address of an SNA CU is configured as 0x00, irrespective of the port's connection mode or type.

Table 14-6 Configurator Error Messages (cont.)

Message	Problem
Invalid Group Poll Addr	1) You tried to configure a group address on a point-to-point link. 2) A group address of 0xFF is configured on a multi-point link.
Invalid SSAP	The SSAP address does not fall in the range 0x04-0xFE (inclusive).
Invalid DSAP	The DSAP address does not fall in the range 0x04-0xFE (inclusive).
Invalid N2	The N2 does not fall in the range 1-20 (inclusive).
Invalid N3	The N3 does not fall in the range 1-20 (inclusive).
Invalid DLCI	The DLCI does not fall in the range 16-1022 (inclusive).
Invalid RW	The RW does not fall in the range 1-128 (inclusive).
Invalid TW	The TW does not fall in the range 1-128 (inclusive).
Invalid XID	The SNA CU is either type PU1 or PU2.1 and you tried to configure XID. (The XID can be configured only for PU2.0 devices.)
No Frame Relay/X.25 Port Configured	You did not configure a frame relay port or an X.25 port prior to attempting this selection.
No SDLC Ports Configured	You did not configure an SDLC port prior to attempting this selection.
No Tab/Space	There are spaces orTAB characters in the name fields.
Ti<T1	The inactivity timer is smaller than the T1 acknowledgment timer.

Table 14-6 Configurator Error Messages (cont.)

Message	Problem
X121 Address Does Not Exist	1) The assigned X.121address is not numeric or exceeds 15 digits in length. 2) An X.121 address has not been assigned. 3) The X.121 address assigned is not defined in the X.25 Concentrator Routing table.
Asterisk (*) Symbol	An asterisk is displayed on the SNA CU Configuration screen for the first entry that has caused any of the errors in this table.

THE ETHERNET BRIDGE APPLICATION

15

■ INTRODUCTION

The *DYNASTAR* Ethernet bridge application provides Ethernet-to-Ethernet remote bridging (IEEE 802.1d) using the spanning tree protocol to provide advanced bridging functions. The connection between a pair of bridges can be over a high-speed T1 (ATM) circuit, a switched circuit over an X.25 packet network, or over a frame relay connection.

SPANNING TREE OVERVIEW

The *DYNASTAR* sends and receives data messages called Bridge Protocol Data Units (BPDUs) at a regular, user-defined interval and calculates the best loop free path throughout the network. Switches in the network do not forward BPDUs, but use these frames to build and maintain loop free paths.

Using the BPDU information, the *DYNASTAR* determines if multiple active paths exist between switches and blocks the least desirable redundant paths so loops are not created. If a loop were to exist in a network, there is a potential for duplicate messages with switches ‘learning’ the same Media Access Control (MAC) addresses on multiple ports. This condition could result in network instability. For additional information on the Spanning Tree Protocol, see AppendixF.

The bridge is self-configuring. On power-up, the bridge learns the location of all nodes (that is, LAN workstations) by examining network traffic and building address tables.

It then determines the best loop-free path for sending information across complex network topologies and allows for bridging traffic over all available paths while ensuring that undesirable loops are not created. If a link fails, an automatic reconfiguration function calculates the next best route and unblocks the appropriate path bridging traffic over another link. The bridge uses the Ethernet address field to filter local frames and forwards frames to remote or unknown addresses.

NOTE: Traffic cannot be bridged between Ethernet and Token Ring LANs.

In addition, the *DYNASTAR* provides the following bridge features:

- All *DYNASTAR* synchronous connections are capable of carrying bridge and router (brouter) traffic. When the *DYNASTAR* is configured as a brouter, IP/IPX traffic is automatically routed. All other traffic, such as DECnet, SNA, XNS, and OSI, is bridged.
- Bridge operation is also supported over dial entries. This feature lets you place a call manually to temporarily connect a pair of remote LANs. See the configuration of the PPP dial directory in Chapter 10, *The PPP Application*, for details on implementing this feature.
- The bridge can filter traffic based on the protocol ID or the MAC address.

■ CONFIGURING THE ETHERNET PORT

A few parameters must be set for your Ethernet port. The built-in Ethernet port is port 0.

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) appears.

2. Select **Port**.

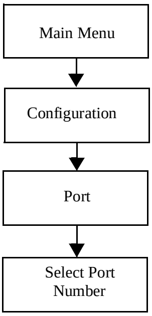
✓ A list of available ports appears.

3. Enter the number of the Ethernet port at the **Enter port number** prompt.

✓ A menu similar to the one in Figure 15-1 appears, showing the port parameters that are currently set for the port.

```
                    ***Ethernet Interface Parameters***
Port: 0 On-board Ethernet                         Last changed: 4-23-02  08:00:45

    | - Press <RET> to toggle values - | | - Type in values. Max chars shown in () - |

Port type: ethernet                              Port name: Ethernet              (14)

MAC address: 00206100399c

Traffic types permitted to/from LAN
        IP Routing:                 Y
        IPX Routing:                N
        Ethernet Bridging:          Y
        OSI Routing:                N

LAN Speed:                          10 Mb/s




_______[DynaStar  dc00399c]_______               Process selections: (Y/N) Y
Use TAB & CURSOR keys to move among fields. Press ESC to  abort command & exit.
```

Figure 15-1 Ethernet Port Configuration Screen



4. In the **Port name** field, give the port a name that will help you identify this port. This name will subsequently appear in any list of the ports, such as the list from which you select a port to configure.

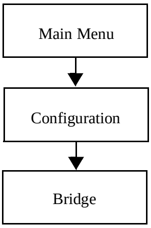
5. In the **Traffic types…** field, toggle to indicate what types of traffic will be allowed.

> **NOTE:** The MAC address is preassigned and cannot be changed.

6. When you have completed your configuration, enter **Y** and press **<return>** at the **Process selections** prompt to save and quit.

7. Press **<ESC>** twice to return to the Configuration Commands menu.

8. Select **Bridge**.



9. The Bridge Commands menu, shown in Figure 15-2, appears.

```
***Bridge Parameters***

1 - Ethernet Bridge parameters
2 - Ethernet Bridge filters

Enter command number:

_______[DynaStar  dc000345]_______
Terminate input with <RET>.                Press ESC to return to previous menu.
```

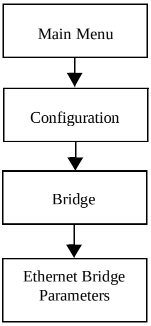
Figure 15-2 Ethernet Bridge Commands Menu

10. Select **Ethernet Bridge parameters**.

✓ The Ethernet Spanning Tree Bridge Parameters screen, shown in Figure 15-3, appears.

```
                ***Ethernet Spanning Tree Bridge Parameters***
                                              Last changed: 4-23-02  08:00:45


   IEEE 802.1   Bridge Priority:          32768    (0 to 65535)
                Bridge Ageing Time:       5        (1 to 255 minutes)
                Bridge Hello Time:        2        (1 to 10 seconds)
                Bridge Forward Delay:     15       (4 to 30 seconds)
                Bridge Maximum Age:       20       (6 to 40 seconds)



                                                 Process selections: (Y/N) Y
_______[DynaStar  dc000345]_______
Use TAB & CURSOR keys to move among fields. Press ESC to  abort command & exit.
```

Figure 15-3 Ethernet Bridge Parameters Menu



11. Set the parameters to appropriate values. Parameters are explained in Table 15-1.

12. When you have completed your configuration, enter **Y** and press **<return>** at the **Process selections** prompt to save and quit.

13. If your bridge traffic will be using an X.25 link, you must continue your configuration as explained in the section *Bridge and Router Configuration* in Chapter 6.

If your bridge traffic will be using a frame relay connection, you must continue your configuration as described in Chapter 8, *The Frame Relay Application*.

If your bridge traffic will be using the Managed Ethernet Switch, you must continue your configuration as described in Chapter 18, *Ethernet Switch Module.*

Table 15-1 Bridge Parameter Values

Parameter	Description	Default
Bridge Priority	Used by the IEEE 802.1d spanning tree algorithm to determine the root of the interconnected network. Bridge priority provides a means of assigning a relative priority to each bridge within the set of bridges in the bridged LAN.	0-65535 32768=default
Bridge Aging Timer	Value that the bridge uses to automatically remove end stations (i.e., Ethernet addresses) after the last activity from/to the end station. The aging timer allows an end station to move to another LAN or become inactive.	1-255 minutes 5=default
Bridge Hello Time	The amount of time between the transmission of configuration bridge PDUs on any port. The hello time is also used when this bridge is attempting to become the root.	1-10 seconds 2=default
Bridge Forward Delay	Controls how long the bridge waits after any state or topology change before forwarding the information to the network.	4-30 seconds 15=default
Bridge Maximum Age	Specifies the age of STP information learned from the network on any port before it is discarded.	6-40 seconds 20=default

■ BRIDGE FILTERING

DYNASTAR bridging lets you block or forward traffic on a protocol-by-protocol basis by screening either the Protocol ID (PID) (reference RFC 1700) or the destination Media Access Control (MAC) address. To configure call blocking or forwarding:

1. From the Main menu, select **Configuration**.

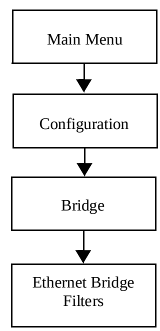
✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. Select **Bridge**.

✓ The Bridge Commands menu (Figure 15-2) is displayed.

3. Select **Ethernet Bridge Filters**.

✓ A screen similar to the one in Figure 15-4 is displayed.




```
                          ***Ethernet Bridge Filters***
                                           Last changed: 4-23-02  08:00:45

  Protocol Name       Block/Forward            PID          MAC Address
 (1-15 characters)      (Toggle)         (?<RET> for list)    (12 Hex)
 1:NOVELL-LAN         Block PID                8137         002061003300
 2:
 3:
 4:
 5:
 6:
 7:
 8:
 9:
10:
11:
12:
13:
14:
15:
Other traffic: Forward

_______[DynaStar  dc000345]_______               Process selections: (Y/N) Y
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 15-4   Ethernet Bridge Blocking and Forwarding

4. In the **Protocol name** column, enter a name that will help you identify the other entries on this line.

5. In the **Block/Forward** column, toggle to select one of the following:
   - Block PID
   - Forward PID
   - Block MAC address
   - Forward MAC address

✓ The cursor moves to the appropriate column: **PID** or **MAC Address** depending on your selection.

6. Fill in the appropriate PID or MAC address.

   NOTE: When you tab to the **PID** field, you can review a list of common PIDs by pressing a question mark (**?**) followed by **<return>** (reference RFC 1700).

7. In the **Other Traffic** field at the bottom of the page, select **Block** or **Forward** to indicate how traffic not specified on this screen will be handled.

8. When your selections are complete, enter **Y** in the **Process selections** field and press **<return>**.

OSI.GATE

■ PRODUCT DESCRIPTION

OSI.Gate is a licensed software application compatible with Software Versions 6.04 and above that can be configured to work on any *DYNASTAR* Ethernet, TCP-IP, or X.25 port. OSI.Gate provides protocol access, concentration, and mediation for Operational Support Systems Network Elements and legacy network managers through modern Telecommunications Management (TMN) compliant systems. The application is available in either a limited or a full version. The limited version supports 10 concurrent X.25 connections. The full version supports 256 concurrent X.25 connections.

BACKGROUND

TMN architecture, the new ITU framework for telecommunications management, supports OSI protocol and was designed to manage high-performance SONET/SDH equipment, already the technology of choice in the worldwide telecommunications market. TMN provides an already accepted means for carriers to integrate their OSS functions, an important factor in a highly competitive market where the quality of service provisioning can distinguish one carrier from another.

The US Telecommunications Reform Act of 1996, in addition to increasing competition, imposed that existing carriers and new competitors make their networks interoperable. Because carriers worldwide are adopting TMN and moving toward compatibility using OSI protocol, existing carriers are compelled to find an inexpensive solution for immediate interoperability with OSI and TMN-based systems, a solution that provides a path to full OSI/TMN compliance over time. OSI.Gate is such a solution.

OSI.Gate software enables the *DYNASTAR* to:

- act as a TL1 converter between TL1, X.25, and TL1 seven-layer OSI
- serve as an OSI transport bridge
- function as an OSI router
- tunnel OSI through a TCP network to OSI managers or elements on either side.

TL1 CONVERTER. As a TL1 converter, the *DYNASTAR* provides communication between network elements that use OSI and legacy network managers that use TL1 protocol to control a variety of older Network Elements (NEs). These legacy NEs and associated management systems will remain essential assets to existing carriers for some time to come. However, as existing carrier networks expand and open to newer OSI-based networks, the conversion of TL1 messages and OSI management messages is critical.

Figure 16-1 portrays the *DYNASTAR* as a TL1 converter that resolves the immediate communication problem between networks based on legacy protocols and networks that have adopted the new protocols slated to become standards.

This gateway converter function provides mediation between a TL1 manager and Network Elements that support the TL1 command set over the seven-layer OSI protocol. Connections can be established over an 802.3 LAN segment or an X.21 physical interface.

As illustrated in Figure 16-2, the *DYNASTAR* removes the payload from X.25 packets. The data is inserted as a TL1 message in a seven-layer OSI packet and sent to its destination.

The TL1 converter function also provides mediation between OSI TL1 managers and legacy network elements. Using OSI ES-IS, IS-IS routing protocol and a TID Address Resolution Protocol (TARP) engine, OSI.Gate automatically discovers Network Elements and translates TL1 Terminal ID (TID) addresses to Network Service Access Points (NSAPs) required for routing within the network.

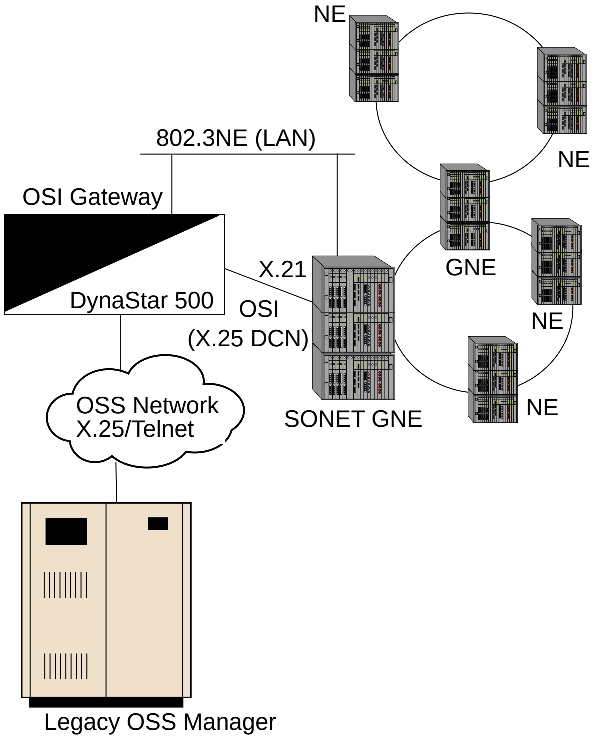


Figure 16-1 TL1 Conversion between Legacy OSS Manager and OSI Network Elements

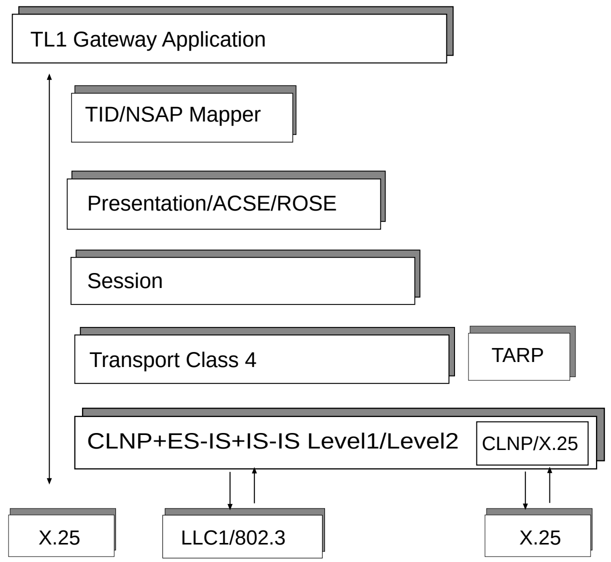


Figure 16-2 TL1 Conversion between Legacy Protocols and OSI

OSI TRANSPORT BRIDGE. As an OSI transport bridge between WAN and LAN ports, the *DYNASTAR* can connect multiple remote sites communicating over X.25 links to an OSI network management station with limited X.25 access links. The *DYNASTAR* thus overcomes the need for a costly X.25 concentrator and eliminates the potential for bottlenecks that are common with concentrators. Operating over the Ethernet port (Port 0), a *DYNASTAR* acting in this capacity also frees the OSI manager's X.25 links for other traffic.

Figure 16-3 shows the *DYNASTAR* in a transport bridge scenario. As Figure 16-4 illustrates, the lower three layers of the packets are replaced, and the Transport class is modified as packets are transferred across the bridge.

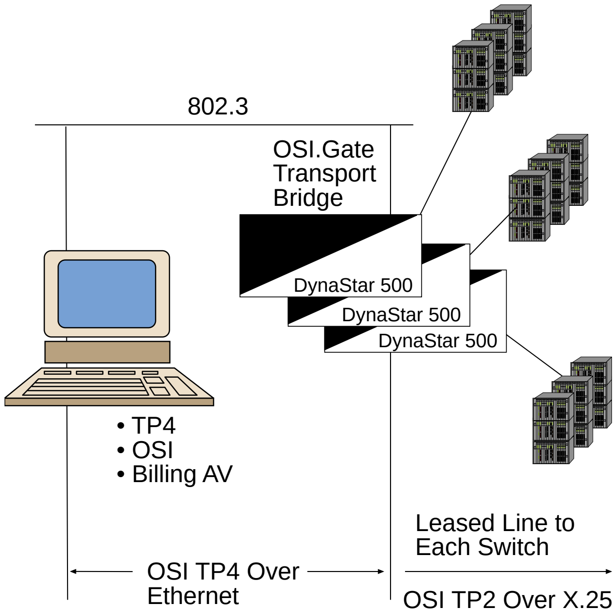


Figure 16-3 The *DynaStar* as a LAN/WAN Transport Bridge

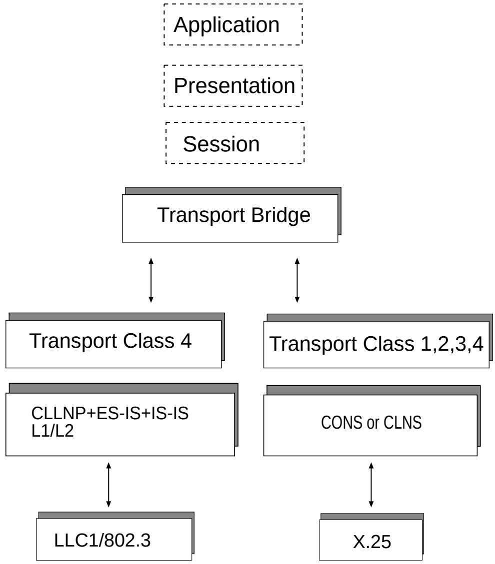


Figure 16-4 Transport Bridge and Protocol Layers

OSI ROUTER. A *DYNASTAR* with OSI.Gate installed supports full OSI Routing for both End System to Intermediate System (ES-IS) transmissions and Intermediate System to Intermediate System (IS-IS) transmissions (including level I and level II areas).

Figure 16-5 shows the *DYNASTAR* operating as an OSI router.

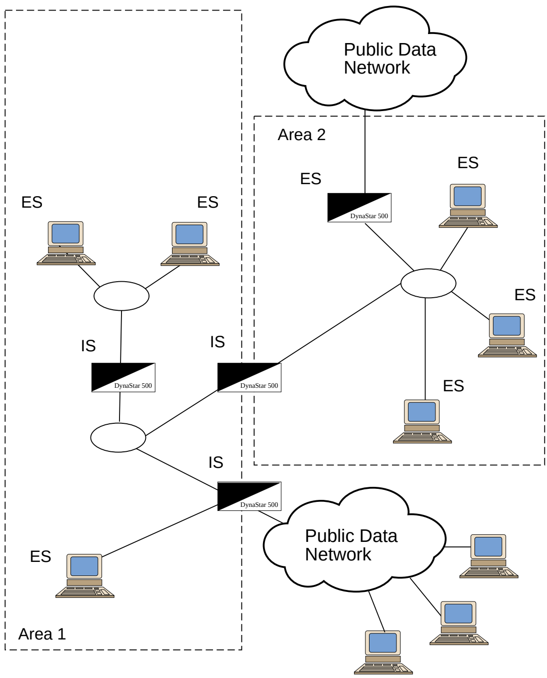


Figure 16-5 The *DYNASTAR* as an OSI Router

OSI TUNNELING. OSI.Gate supports tunneling of OSI packets through TCP/IP networks. This serves as a "full migration" feature useful to existing carrier networks that are beginning to incorporate OSI-compliant equipment. The feature will also be useful to newer, OSI-based networks with equipment connected via TCP/IP.

Figure 16-6 illustrates OSI tunneling. Figure 16-7 shows how X.25 layers are handled in the tunneling process. As the diagram indicates, X.25 data passing through an OSI/TCP network is stripped from the X.25 packet, encapsulated in OSI packets, and transported over TCP/IP.

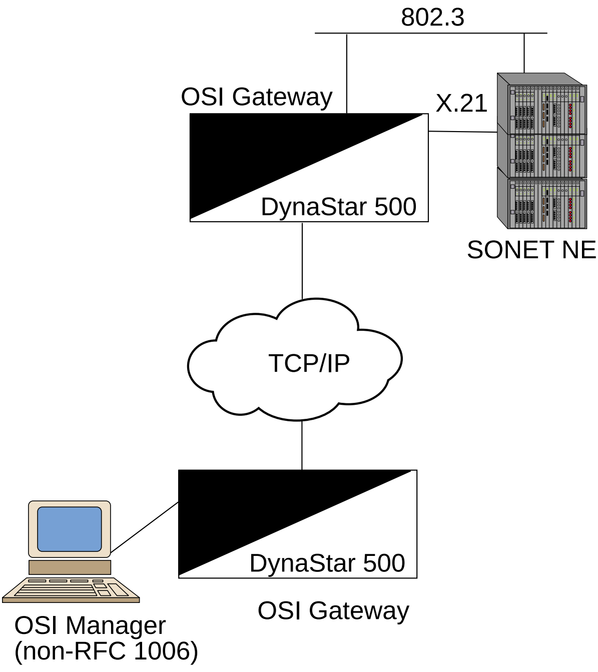


Figure 16-6 OSI Tunneling

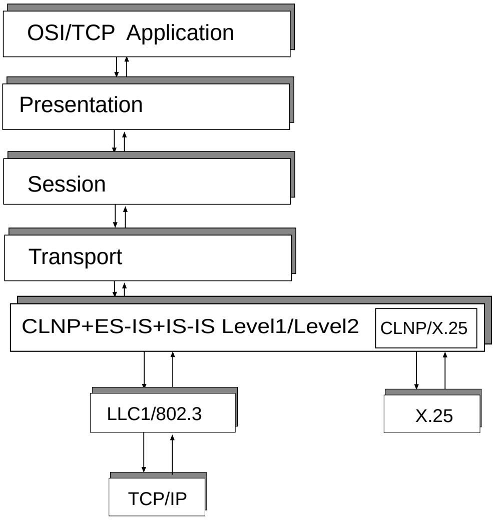


Figure 16-7 X.25 Layers and OSI Tunneling

■ Hardware and Software Requirements

OSI.Gate requires 16MB of RAM and operates with Software Version 6.04 or later. The application is activated with a key that locks to the MAC address of your *DynaStar*.

Obtaining a Key

To obtain a key, complete and submit the forms provided at the time you purchased OSI.Gate to the address or the fax number indicated on the form. A key will be returned to you.

■ The First Time You Use OSI.Gate

Once you receive the software activation key, you must enter it on the Applications menu. To enter the key:

1. From the Main menu, select **System Functions**.

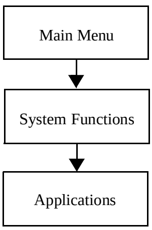
✓ The System Commands menu (Figure 3-13) is displayed.

2. Select **Applications**.

✓ The Applications menu (Figure 16-8) is displayed.

3. In the field **DynaStar OSI.Gate Application**, select **Limited**.

✓ The field **Enter key** appears to the right.




```
                              *** Applications ***

Serial Number:        3df2     ROM Installed:  3.9     NCSI_WAN Required:    3.2
Private MIB Version:  4.2      ROM Required:   3.9     INT14WAN Required:    1.0
                                X.25 Version:  2.0     OSI Version:          1.00

File                 Date      Time   Blocks  File              Date     Time   Blocks
DOWNLOAD.BIN*10-09-02 11:27  3973    ATICLOAD.BIN    <not loaded>
ETH8LOAD.BIN    10-09-02 11:27   174    QPMLOAD.BIN    <not loaded>
DMAPLOAD.BIN    10-09-02 11:27   196    No binary config file loaded
QUADLOAD.BIN    10-09-02 11:27   333
816PLOAD.BIN    10-09-02 11:27   319
T1E1LOAD.BIN    10-09-02 11:27   331
DBRILOAD.BIN    10-09-02 11:27   278
   * running version          5253 KB free
                                      Toggle with <RET>        Type in value
                                         --------------          --------------
DynaStar OSI.Gate Application               Limited

Auxiliary Functions                        Temp                      Save Setting
                                           Sensor                    when Exit
Active (Y/N):                                N                           N

_________[DynaStar_3df2]__________
Use TAB & CURSOR keys to move among fields. Press ESC to return to previous menu.
```

Figure 16-8   The Applications Menu

4. Enter the Limited key you received and press **<return>.**

✓ If you have purchased the limited version of OSI.Gate, it is now active and you may skip to step 7. If you purchased the full version, continue with step 5.

5. Place the cursor in the field **DynaStar OSI.Gate Application** again. This time, select **Full**.

✓ The field **Enter key** appears to the right.

6. Enter the Full key you received and press **<return>**.

7. Reboot the *DYNASTAR* with the Warm Restart command from the System Commands menu.

✓ The version of OSI.Gate you purchased is now active on the *DYNASTAR* and is ready to be configured as described in the sections that follow.

DEACTIVATING OSI.GATE

Deactivate either version of OSI.Gate by repeating the activation procedure described in the previous section. Deactivating OSI.Gate has no effect on any other features or functions of the *DYNASTAR*.

TURN ON OSI ROUTING

The *DYNASTAR* can route OSI traffic only if routing has been enabled. To turn on OSI routing:

1. From the Main menu, select **Configuration**.

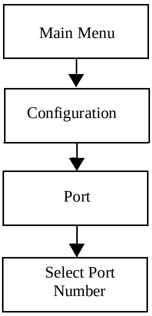
✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. Select **Port**.

✓ The Configure Port menu, which lists available *DYNASTAR* ports, is displayed.

3. Select any Ethernet port.

✓ The Ethernet Port Configuration menu (Figure 16-9) is displayed.




```
                    ***Ethernet Interface Parameters***
Port: 0 On-board Ethernet                          Last changed: 4-23-02  08:00:45

   | - Press <RET> to toggle values - | | - Type in values. Max chars shown in () - |

Port type: ethernet                            Port name: Ethernet            (14)

MAC address: 00206100399c

Traffic types permitted to/from LAN
     IP Routing:                 Y
     IPX Routing:                Y
     Ethernet Bridging:          Y
     OSI Routing:                Y




_______[DynaStar dc00399c]_______              Process selections: (Y/N) Y
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 16-9 Ethernet Port Configuration Screen

4. In the field **OSI Routing**, select **Y**.
5. In the field **Process selections**, enter **Y** and press **<return>**.

✓ OSI routing is enabled.

■ CONFIGURE X.25 VIRTUAL CIRCUITS

When OSI traffic traverses an X.25 network, the *DYNASTAR* redirects the traffic to the various OSI applications using virtual circuits that have been configured to handle a specific application. Currently, Switched Virtual Circuits (SVCs) can be associated with an OSI application. Permanent Virtual Circuits (PVCs) will be supported in the future. The following procedure describes how to configure these virtual circuits. Virtual circuit parameters are defined in Table 16-1.

1. From the Main menu, select **Configuration**.

- ✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. Select **X.25**.

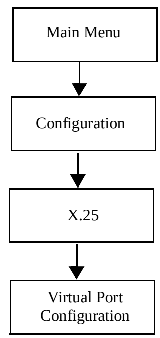
- ✓ The X.25 Parameters menu (Figure 6-3) is displayed.

3. Select **Virtual Port Configuration**.

- ✓ The Virtual Port Configuration Table (Figure 16-10) is displayed. You can configure up to 15 different virtual circuits for OSI use on this table.

```
        *** Virtual Port Configuration Table (TIDMUX, CONTACT, OSI) ***
                                           Last changed:  4-23-02 9:44:30
   Service            X.25 NUA          APP           LCN #        Port #
   (Toggle)           (SVC only)        (Toggle)            (PVC only)
 1:
 2:
 3:
 4:
 5:
 6:
 7:
 8:
 9:
10:
11:
12:
13:
14:
15:

_______[DynaStar-Dc00375]_______                    Process entries (Y/N):Y
In Service field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.  Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields.Press ESC to abort command & exit.
```

Figure 16-10 Virtual Port Configuration Table



4. For each service being configured, toggle to select **SVC** in the **Service** field.

5. Tab to the APP field and toggle to select the type of OSI application to be provided on the virtual circuit.

NOTE: The **LCN #** (Logical Channel Number) and the **Port #** (X.25 trunk number) fields are intended for use with PVCs and are not active at this time.

6. Fill in the field **X.25 NUA**. The meaning of this field depends on the application you have selected. See Table 16-1 for more information.

7. In the field **Process Entries**, enter **Y** and press **<return>**.

✓ You return to the X.25 Commands menu.

Table 16-1 OSI X.25 Virtual Circuit Parameters

Parameter	Description	Value
Service	Select Switched Virtual Circuit (SVC). Note: Permanent Virtual Circuits (PVCs) will be supported in a future release.	SVC PVC (not yet available)
X.25 NUA	This field is valid only if Service type is SVC. For TL1,enter the X.121 address of the *DYNASTAR*'s TL1 gateway. For CLNS, TxIS, RxIS, or CONS, enter the X.121 address that a Network Element uses to communicate with the *DYNASTAR* across an X.25 link.	Address
APP	Toggle to select TL1 (TL1 3/7 conversion), CONS (X.25 connection-oriented network service), CLNS (X.25 connectionless network service), or TxIS/RxIS (transmit or receive ES-IS, IS-IS over X.25) as the application type.	TL1 CONS CLNS TxIS/RxIS
LCN #	This field is valid only if Service type is PVC. Logical Channel Number of the X.25 virtual circuit on which the OSI service is defined.	Not currently active
Port #	This field valid only if Service type is PVC. Inbound trunk of the *DYNASTAR* on which the OSI service is defined.	Not currently active

■ Configure TL1 Converter

The previous section described the steps needed to configure the TL1 converter when legacy TL1 managers (using X.25) are used to communicate with the newer OSI Network Elements. This section explains the steps you use when an OSI TL1 manager needs to communicate with legacy Network Elements (using X.25).

1. From the Main menu, select **Configuration**.

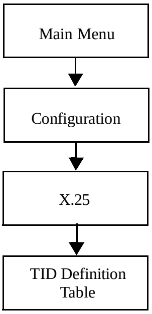
✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. From the Configuration Commands menu, select **X.25**.

✓ The X.25 Parameters menu (Figure 6-3) is displayed.

3. Select **TID DefinitionTable** .

✓ The TID Definition Table, as shown in Figure 16-11, is displayed.




```
                 *** TID Definition Table (TIDMUX, CONTACT, OSI) ***
                                                  Last changed:  4-23-02 9:44:30
   APP              TID               X.121 Address       Port #        TL1/SNMP
   (Toggle)      (22 alphanumeric)   (1-15 BCD)                        (Contact Only)
 1:  OSI-X25      TID00123456          893456                              TL1
 2:  OSI-X25    TID00DYNASTAR          878656
 3:
 4:
 5:
 6:
 7:
 8:
 9:
10:
11:
12:
13:
14:
15:

_______[DynaStar-Dc00375]_______                        Process entries (Y/N):Y
In the TID field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.  Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields.Press ESC to abort command & exit.
```

Figure 16-11 TID DefinitionTable

4. In the APP field, select **OSI-X25**.

5. In the TID field, enter a Target ID that can be received in data packets from the TL1 manager over OSI.
6. In the X.121 address field, enter the X.121 address of the Network Element that corresponds to the TID entered in the TID field. (No entry is required in the Port # field.)
7. When your entries are complete, save them by entering **Y <return>** in the Process Entries field.

✓ You return to the X.25 Parameters menu.

NOTE: When using the TL1 converter for conversion from OSI to X.25, you must set the System Type to End System or Intermediate System + End System. To set the System Type, please refer to the section *Define OSI Parameters*.

■ Configure Static Routes

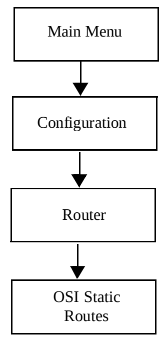
If OSI.Gate will be transporting data via a WAN connection, configure OSI Static Routes for all devices connected over the WAN. The following procedure explains how to configure these routes. Static route parameters are described in Table 16-2.

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. Select **Router**.
3. The Router Commands menu (Figure 12-2) is displayed.
4. Select **OSI Static Routes**.

✓ The OSI Static Routes screen, shown in Figure 16-12, is displayed.




```
                         *** OSI Static Routes ***
                                      Last changed:  4-23-02 9:44:30
CLNS/CONS           NSAP                                X.121 Address
 (toggle)          (40 Digits)                          (14 Digits)
   1:CLNS    abcdef000000000012120000000012312300001d          45678
   2:CONS    abcfed566777123123123000000123123123121d          999765
   3:CLNS
   4:CLNS
   5:CLNS
   6:CLNS
   7:CLNS
   8:CLNS
   9:CLNS
 10:CLNS
 11:CLNS
 12:CLNS
 13:CLNS
 14:CLNS
 15:CLNS
_______[DynaStar-Dc00375]_______                  Process OSI Routes (Y/N):Y
In NSAP address field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value.  Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields.Press ESC to abort command & exit.
```

Figure 16-12 OSI Static Routes Menu

5. Select CLNS or CONS to specify the type of network service used on theWAN.

6. Fill in the full 40 digits of the NSAP in the OSI network.

7. Enter the destination's X.121 address.

8. In the **Process OSI Routes** field, enter **Y** and press **<return>**.

✓ You return to the Router Commands menu.

Table 16-2 OSI Static Route Parameters

Parameter	**Description**
CLNS/CONS	Toggle to indicate whether the X.25 network uses Connection-Oriented (CONS) or Connectionless (CLNS) X.25 link protocol.
NSAP	Enter the 40 digits of the NSAP address for the destination device in the OSI network.
X.121 Address	Enter up to 14 digits for the X.121 address of the device.

■ CONFIGURE OSI TUNNEL ROUTES

This feature is used when TL1 messages in OSI packets must be transported across a TCP/IP network between Network Elements and OSI managers.

1. From the Main menu, select **Configuration**.

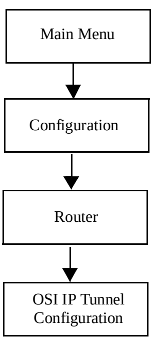
✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. From the Configuration menu, select **Router**.

✓ The Router Commands menu (Figure 12-2) is displayed.

3. From the Router menu, select **OSI/IP Tunnel Routes**.

✓ The OSI/IP Tunnel Configuration screen, shown in Figure 16-13, is displayed. A maximum of five tunnels can be configured.




```
                    *** OSI IP Tunnel Configuration ***
                                    Last changed:  4-23-026 9:44:30
SEND/RECV          IP Address            Socket              NSAP
 (toggle)            x.x.x.x                               40 Hex Digits
   1:SEND        123.123.123.123          3400
   2:RECV        234.234.234.234          5500
   3:SEND
   4:SEND
   5:SEND

_______[DynaStar-Dc00375]_______              Process Tunnel Routes (Y/N):Y
To change or add entry, enter new value.        Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 16-13 OSI IPTunnel Configuration Menu

4. In the SEND/RECV field, toggle to choose between SEND/RECV. If the *DYNASTAR* is the source end of the

tunnel choose **SEND**. If the *DYNASTAR* is the destination end of the tunnel, choose **RECV**.

5. In the IP Address field, enter the IP address of the *destination* end of the tunnel.
6. In the Socket field, enter the socket of the *destination* end of the tunnel.
7. In the Process Tunnel Routes field, enter **Y <return>**.

✓ Your OSI tunnel configuration is complete.

Table 16-3 OSI IPTunnel Parameters

Parameter	Description
SEND/RECV	Toggle to indicate if the *DYNASTAR* is the source end of the tunnel or the destination end of the tunnel.
IP Address	Indicate the IP address of the destination end of the tunnel. This should be the same in both ends of the tunnel.
Socket	Indicate the socket of the destination end of the tunnel. This should be the same in both ends of the tunnel for the corresponding IP address.
NSAP	40 digits. This field is for future use.

■ DEFINE OSI PARAMETERS

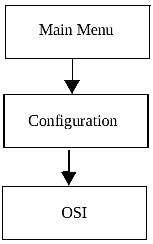
On the OSI Configuration menu, define system type, address, and, if needed, routing for the *DYNASTAR*. The following procedure describes system configuration. OSI system parameters are defined in Table 16-4.

To configure OSI parameters for the *DYNASTAR*:

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. Select **OSI**.



✓ The OSI Configuration menu (Figure 16-14) is displayed.

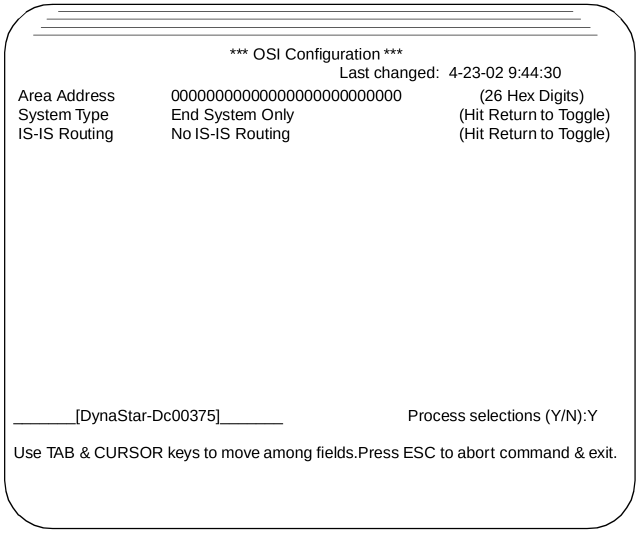


Figure 16-14 OSI Configuration Menu

3. Fill in the area address within the OSI network. Be sure to type in all 26 hex digits.
4. Select the system type.
5. Select the routing type. (This field is not active if you have selected **End System** as the system type.)
6. Enter **Y** in the **Process Selections** field and press **<return>**.

✓ The screen shown in Figure 16-15 appears and displays the message that the *DYNASTAR* must be rebooted for your configuration to take effect.

7. To reboot the *DYNASTAR*, enter the unit's password in the space provided and press **<return>**. Or abort the configuration and the restart by pressing **<esc>**.

```
*** MESSAGE SCREEN ***

Changes in the OSI Configuration require the system to be rebooted.
Press ESC to abort or enter the Current Password to save changes and
reboot the system.

          Enter Current Password:  _______________

_______[DynaStar-Dc00375]_______
Terminate input with <RET>.                Press ESC to abort command & exit.
```

Figure 16-15 Reboot Message Screen

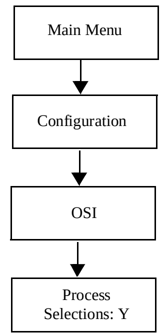


Table 16-4 OSI Configuration Parameters

Parameter	Description	Values
Area Address	Enter the NSAP address defined for the *DynaStar* within the OSI network. Highlight the field and type your entry in full, even if there are digits that do not change or trailing zeroes.	26 hex digits All zeroes (default)
System Type	Toggle to indicate the *DynaStar*'s position in the network. This determines how the *DynaStar* handles routing.	End System Only (default) Intermediate System Only End System + Intermediate System

Table 16-4 OSI Configuration Parameters (cont.)

Parameter	Description	Values
IS-IS Routing	This field applies only to intermediate systems. Toggle to indicate the type of OSI routing to be applied. Note: If you have chosen End System Only as the System Type, this field is fixed at No IS-IS Routing.	No IS-IS Routing (Default) Level 1 Routing Level 1 + Level 2 Routing

■ ADVANCED DEBUGGING

Special status screens, covered in the next sections, allow you to display contents of various OSI routing tables as well as manual routing entries configured on the *DYNASTAR*.

VERIFYING THE OSI ROUTING TABLE

A special table allows you to check the NSAPs that can be reached through the Ethernet interface. Depending on the system type specified on the OSI Configuration menu (Figure 16-14), the different End Systems, Intermediate Systems, or both that the *DYNASTAR* has discovered are displayed. To access the menu:

1. From the Main menu, select **Status**.

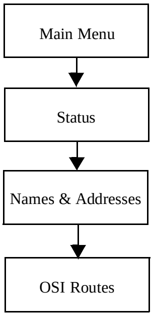
✓ The Status Commands menu (Figure 3-7) is displayed.

2. Select **Names and Addresses**.

3. The Names and Addresses menu (Figure 12-7) is displayed.

4. Select **OSI routes**.

✓ The OSI Routes menu (Figure 16-16) is displayed. All configured routes are summarized on this menu.




```
                              *** OSI Routes ***

Type    NSAP    (ESI)   or   Title   (ISI)                 SNPA
ISI     39840f80000000000000000000000e44026c00             00000e44026c

_________[DynaStar_3df2]__________
Use XOFF <CTRL-S> and XON <CTRL-Q>       Press <RET> for update.
              to control scroll.         Press ESC to return to previous menu.
```

Figure 16-16 OSI Routes Menu

THE OSI CONSOLE SCREEN

The OSI Console screen is used for advanced debugging. Only qualified service personnel should use this screen. To access the screen:

1. From the Main menu, select **Status**.

✓ The Status Commands menu (Figure 3-7) is displayed.

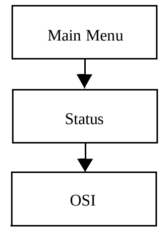
2. Select **OSI**.

✓ The OSI Console screen is displayed. The words *OSI operator console* appear at the top of the screen. (See examples for various commands in Figure 16-17 through Figure 16-22.)

3. Enter commands at the > prompt. Debugging commands are given in Table 16-5.

Table 16-5 Console Debugging Commands

Command	Meaning
tarp tdc dump	Displays the contents of the tarp table. Check the contents to see if the system has detected the NSAP for the TID you are trying to reach.
tarp tdc flush	Clears the tarp tables.
tarp mat dump 1	Displays the manual adjacency table (MAT) forTARP. The MAT includes NSAPs that are added manually to the TARP table. Note: Entries in the *DYNASTAR* Static Routes table are reflected in the MAT.
tarp get c<TID> *(where <TID> is the alpahnumeric name of the Target ID)*	Checks to see if a specific TID can be reached; that is, whether the NSAP can be resolved. The TID for the *DYNASTAR* is “TID00xxxx”, where “xxxx” is the last four digits of the MAC address of the *DYNASTAR*.
e2i sh gri 41 2 -1	Displays the global routing table, which contains all the routes discovered through ES-IS protocol as well as static routes configured through the Static Routes menu.
e2i sh isi 41 2 -1 a	Displays the routing table containing all the discovered Intermediate Systems.
vary sap 69 trace on	Provides a real-time trace of TL1 transactions within the OSI stack. To turn off the trace, enter “vary sap 69 trans off”.




```
*** OSI ***

===================
OSI operator console
===================
-> tarp tdc dump
bc55[2900] TARP_TDC_READ_CNF [req was TDC Dump]
bc55[2900]    result:   OK[0]
bc55[2900]    EntryID:  0
bc55[2900]    Net:      39840f8000000000000000000000000e44026c00
bc55[2900]    TID:      fatigues [66756a69747375]
bc55[2900]    tar-pro:  fe
bc55[2900] TARP_TDC_READ_CNF [req was TDC Dump]
bc55[2900]    result:   NOMOREENTRY[1]
bc55[2900]    ------ TDC Dump done ---------------




_________[DynaStar_3df2]__________
Use XOFF <CTRL-S> and XON <CTRL-Q>        Press <RET> for update.
                 to control scroll.       Press ESC to return to previous menu.
```

Figure 16-17 Sample Contents of TARP Table

```
*** OSI ***

===================
OSI operator console
===================
-> tarp tdc flush
bcbc[2900] TARP_RESULT_CNF [req was TDC Flush]
bcbc[2900]    result:   OK[0]
->




_________[DynaStar_3df2]__________
Use XOFF <CTRL-S> and XON <CTRL-Q>        Press <RET> for update.
                 to control scroll.       Press ESC to return to previous menu.
```

Figure 16-18 Results of Flush Command

```
                              *** OSI  ***


===================
OSI operator console
===================
-> tarp mat dump 1
bc6e[2900] TARP_MAT_READ_CNF [req was MAT Dump]
bc6e[2900]    result:   OK[0]
bc6e[2900]    TAbleID:  1
bc6e[2900]    EntryID:  0
bc6e[2900]    Net:      39840f80000000000000000000000e44026c1d
bc6e[2900] TARP_MAT_READ_CNF [req was MAT Dump]
bc6e[2900]    result:   OK[0]
bc6e[2900]    TAbleID:  1
bc6e[2900]    EntryID:  1
bc6e[2900]    Net:      39840f80000000000000000000000e44026caf
bc6e[2900] TARP_MAT_READ_CNF [req was MAT Dump]
bc6e[2900]    result:   NOMOREENTRY[1]
bc6e[2900]    ------ MAT Dump done ---------------

_________[DynaStar_3df2]__________
Use XOFF <CTRL-S> and XON <CTRL-Q>        Press <RET> for update.
              to control scroll.          Press ESC to return to previous menu.
```

Figure 16-19 Sample Contents of MAT Table

```
                              *** OSI  ***


===================
OSI operator console
===================
-> tarp get cdynastar1
bc84[2900] TARP_GET_NSAP_CNF [req was GetNsap]
bc84[2900]    result:   OK[0]
bc84[2900]    Net:      39840f80000000000000000000000e44026c00
bc84[2900]    TID:      dynastar1 [66756a69747375]
bc84[2900]    origin:  From TDC

_________[DynaStar_3df2]__________
Use XOFF <CTRL-S> and XON <CTRL-Q>        Press <RET> for update.
              to control scroll.          Press ESC to return to previous menu.
```

Figure 16-20 Resolution of the TID dynastar1

```
*** OSI ***

===================
OSI operator console
===================
-> e2i sh gri 41 2 -1
bc9a[4113] Routing: Command=0012
bc9a[....] Entry=0 Nsap=39840f8000000000000000000002061003c541d Subn=1 0
bc9a[....] Parm=(4 1 4 0 1)
bc9a[....] Entry=1 Mask=ffffffffffffffffffffffffffffffffffffffff
bc9a[....] Nsap=39840f8000000000000000000000000e44026c1d Subn=2 0 Parm=(0 0 0
0
bc9a[....] 1) Snpa=a44477711110
bc9a[....] Entry=ff Mask= Nsap= Subn=0 0 Parm=(0 0 0 1 1)
bc9a[....] Summary=(3 3)

_________[DynaStar_3df2]__________
Use XOFF <CTRL-S> and XON <CTRL-Q>        Press <RET> for update.
                  to control scroll.      Press ESC to return to previous menu.
```

Figure 16-21 Sample Display of Global Routing Table

```
*** OSI ***

===================
OSI operator console
===================
-> e2i sh isi 41 2 -1 a
bcaf[4113] Routing: Command=0015
bcaf[....] Subn=0 0
bcaf[....] Title=39840f8000000000000000000000000e44026c00 Snpa=00000e44026c
bcaf[....] Parm=(60 70)
bcaf[....] Summary=(1 1)

_________[DynaStar_3df2]__________
Use XOFF <CTRL-S> and XON <CTRL-Q>        Press <RET> for update.
                  to control scroll.      Press ESC to return to previous menu.
```

Figure 16-22 Display of Intermediate System Routing Table

EPOS PAD Software

17

EPOS PAD Software

■ Overview

The EPOS-PAD function is designed to handle high-speed connections for transactions such as credit card or smart card authorization. The EPOS PADsoftware can run only on the *DynaStar 100e*, *DynaStar 2000*, *DynaStar 500*, and *DynaStar 5000*; it cannot run on the *DynaStar 100* or the *DynaStar 100i*.

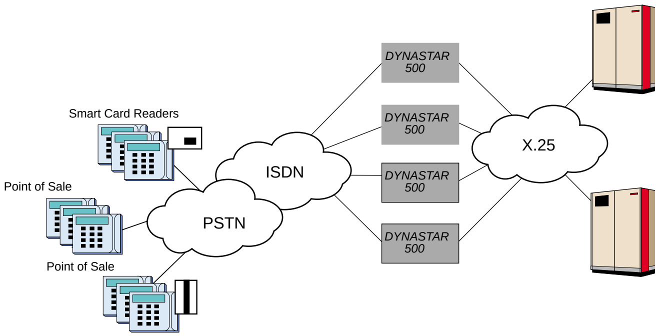


Figure 17-1 Sample EPOS-PAD Application

Figure 17-1 shows a typical EPOS-PAD application. Point-of-sale and smart card terminals connect to the EPOS-PAD function of the *DynaStar* via dial-up services terminated over ISDN. The EPOS-PAD concentrates these connections, establishes an X.25 connection to the host, and continues to pass data in both directions to complete the financial transaction. As described later in this chapter, you can customize the EPOS-PAD settings for various types of lines and assign these settings as profiles. You can also establish modem classes to manage speed, security, and class of service for dial-up connections.

EPOS-PAD hardware provides modem banks for up to 120 concurrent sessions and can terminate dial-up service with up to four primary rate ISDN lines over E1 or T1 facilities.

Please refer to Chapter 19 for information on EPOS status and statistics.

■ THE DIGITAL MODEM SUBSYSTEM

The digital modem subsystem consists of the QPM module, which provides a compact interface to four E1 or T1 lines while allowing individual timeslots to be encoded with V.21 ch 2 modem data. The module accepts up to 15 SIMMs, each of which contains 8 digital modems, for a maximum of 120 digital modems, as shown in Figure 17-2.

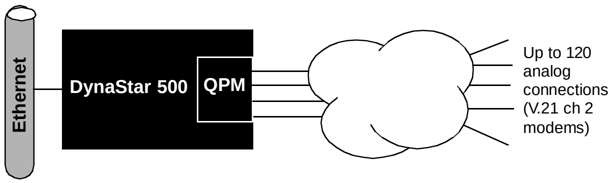


Figure 17-2 ***DYNASTAR 500*** **Digital Modem Subsystem**

The QPM module consists of the following boards:

- One Line Resource Module (LRM)
- One Modem Resource Module (MRM)
- Maximum of 15 Octal Modem SIMM Modules (Octomodems)

LINE RESOURCE MODULE

The Line Resource Module (LRM) is the base module for the QPM subsystem. The LRM supports four line interfaces. The QPM is equipped at the factory to support two or four E1 or T1 lines.

The LRM is a double-sized *DYNASTAR* daughter board that takes up daughter board slots 1 and 2 on the mother board, as illustrated in Figure 17-3.

Modem Resource Module

The Modem Resource Module (MRM) is a daughter board for the LRM. The MRM provides for the physical mounting of up to 15 Octomodem SIMMs. The Octomodems are installed in two banks, a bank of seven that corresponds to slot 1 (closest to the front of the *DynaStar*) and a bank of eight that corresponds to slot 2 (closest to the back of the *DynaStar*). The installation of the module is illustrated in Figure 17-3.

Octal Modem SIMMs

The Octal Modem SIMMs (Octomodems) are 72-pin SIMM modules that each contain eight modem datapumps. The Octomodems are mounted on the QPM, which provides sockets for 15 Octomodems installed in the two banks, for a maximum of 120 modems (8x15). Any number of Octomodems can be installed in either of the two banks in any order up to the maximum allowed. The location of the modules within the QPM subsystem is illustrated in Figure 17-3.

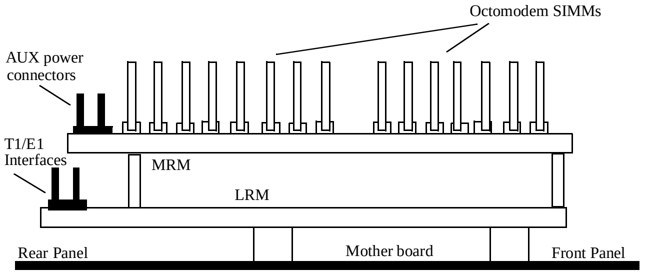


Figure 17-3 QPM Subsystem Installed on *DynaStar* Mother Board

■ Configuring the EPOS-PAD

To configure the EPOS-PAD, you must configure the T1/E1 trunks and their associated incoming phone numbers as well as the B-channels, and you must configure the parameters for the EPOS lines. Figure 17-4 illustrates the steps involved in configuring an ISDN trunk. ISDN Trunk configuration is covered fully in Chapter 9.

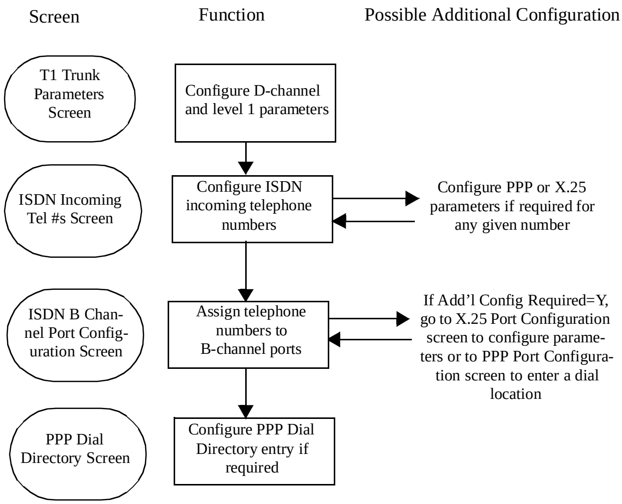


Figure 17-4 ISDN Trunk Configuration

Configuring the EPOS-PAD lines involves

- defining modem parameters, which are stored and assigned as modem classes
- specifying certain PAD values, which are stored and assigned as EPOS profiles
- assigning telephone numbers to the PAD ports to be used for EPOS
- assigning a phone number to the B-channels.

Figure 17-5 illustrates this configuration process. Note that certain portions of the EPOS-PAD configuration can be

performed as part of the ISDN configuration (compare Figure 17-4 to Figure 17-5).

NOTE: Although PPP connections are supported in the *DYNASTAR* implementation of ISDN, they are not supported for EPOS configurations. All EPOS connections are X.25 connections.

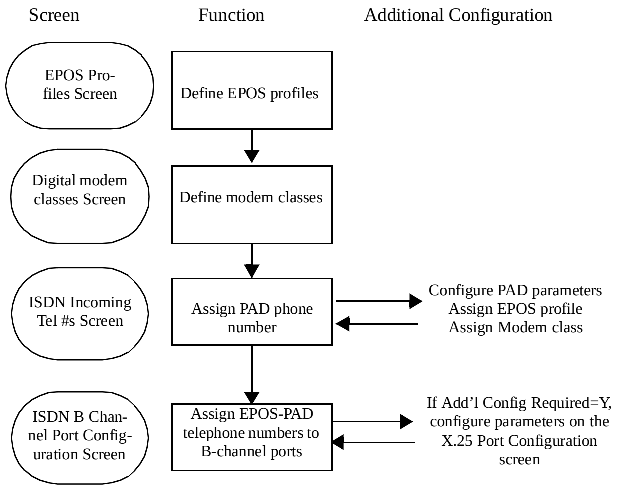


Figure 17-5 Overview of EPOS-PAD Configuration Process

Status and statistic information for the modems and EPOS PADs is explained in Chapter 19, *Monitoring and Statistics.*

CONFIGURING MODEM CLASSES

You can create up to five modem classes for the EPOS-PAD for setting up distinct classes of service, limiting modem types for security, limiting modem types to minimize connection time, and so on. Modem classes also allow you to set up reserve banks to sustain a guaranteed level of service for a particular modem class. Once you have created modem classes, they are assigned to individual lines as described in

the section *Assigning EPOS-PAD Profile and Modem Class and Adjusting PAD Parameters.*

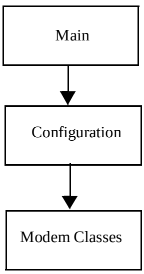
To configure EPOS-PAD modem classes:

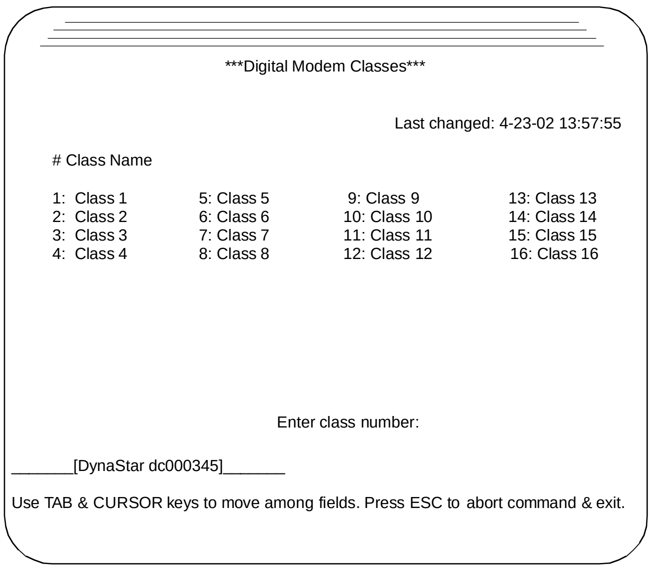
1. From the Main menu, select **Configuration**.

✓ The Configuration Commands Menu (Figure 3-11) is displayed.

2. Select **Modem Classes**.

✓ The Digital Modem Classes menu (Figure 17-6) is displayed.





Digital Modem Classes

Last changed: 4-23-02 13:57:55

\# Class Name

1: Class 1	5: Class 5	9: Class 9	13: Class 13
2: Class 2	6: Class 6	10: Class 10	14: Class 14
3: Class 3	7: Class 7	11: Class 11	15: Class 15
4: Class 4	8: Class 8	12: Class 12	16: Class 16

Enter class number:

_______[DynaStar dc000345]_______

Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.

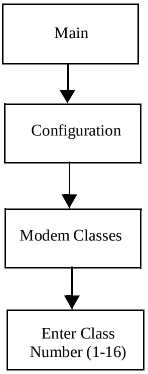
Figure 17-6 Modem Classes Configuration Screen

3. In the **Enter class number** field at the bottom of the menu, type the number of the class you want to configure.

✓ The Digital Modem Configuration menu (Figure 17-7) is displayed.

```
***Digital Modem Configuration***

Press <RET> to toggle values                     Last changed: 4-23-02 13:57:55

    Modem Class:          Class1
    Modem Mode:           Auto
    Modem Type:           V.34
    Parity:               None
    Error Correction:     Auto
    Data Compression:     Auto
    Companding Type:      Auto
    Attenuation:          0x00
    Threshold:            0
    Dial Out Speed:       ISDN64VOICE
    Answer Tone(100ms):   36

                                            Process selections (Y/N):  Y

_______[DynaStar dc000345]_______
Use TAB & CURSOR keys to move among fields.Press ESC to abort command and exit.
```

Figure 17-7 Modem Configuration Screen



4. Set parameters as required for the modem class. Parameters and values are described in Table 17-1.

5. When you have completed your configuration, enter **Y** in the Process Selections field and press **<return>**.

Table 17-1 Modem Parameters

Parameter	Description	Values
Modem Class	Assigns a class name for this modem configuration.	7 characters
Modem Mode	Specifies the mode to be used for modem selection. *Auto* causes modem modulation to be negotiated automatically, starting from the highest modulation (V.34) and working down. If no match is found, the modem hangs up. *Fixed* sets the modem to the modulation specified by the Modem Type parameter on this menu.	Auto (Default) Fixed
Modem Type	Selects the modem type. Note: If you select a specific modem type, the remote modem must also be configured as the same type. V.34 supports the following bit rates (in kbits/sec): 28.8, 26.4, 24.0, 21.6, 19.2, 16.8, 14.4, 12.0, 9.6, 7.2, and 4.8. V.32bis supports the following bit rates (in kbits/sec): 14.4, 12.0, 9.6, 7.2, and 4.8. V.32 supports the following bit rates: 14.4, 12.0, 9.6, 7.2, and 4.8. V.22bis bit rate is 2.4 kbits/sec. V.22 bit rate is 1.2 kbits/sec. V.21 operates at 300 bits/sec	V.34 (default) V.32bis V.32 V.22bis V.22 V.21
Parity	Selects the appropriate parity. *Auto* means that the parity is determined when you enter the auto parity sequence (period followed by <return>).	None (default) Auto, Even Odd, Space, Mark

Table 17-1 Modem Parameters (Cont.)

Parameter	Description	Values
Error Correction	Selects the appropriate error correction protocol. *Auto* attempts to negotiate the use of V.42. Otherwise, no error correction is used. *None* uses no error correction protocol. *V.42* attempts to negotiate use of V.42. Otherwise, the modem disconnects.	Auto (default) None V.42
Data Compression	Selects the appropriate data compression method. *Auto* attempts to negotiate data compression; otherwise, no data compression is used. *None* disables data compression.	Auto (default) None
Companding Type	Selects the appropriate companding method. *Auto* selects a-law companding on E1 interfaces, µ-law companding on T1 interfaces. *a-law* forces a-law companding. *µ-law* forces µ-law companding.	Auto (default) a-law µ-law
Attenuation	For future implementation.	
Threshold	Selects the allocation threshold for the modem class. See *Setting up Reserved Modem Pools* for more information.	0-120 (Default = 0; that is, no minimum pool reserved)

Table 17-1 Modem Parameters (Cont.)

Parameter	Description	Values
Dial Out Speed	Determines B-channel speed and bit usage for the ISDN call set-up. ISDN64VOICE is used for voice calls with out-of-band signalling; ISDN56VOICE is used for voice calls with Robbed-Bit signalling; ISDN56DATA and ISDN64DATA are reserved for future use.	ISDN56VOICE ISDN56DATA ISDN64DATA ISDN64VOICE ISDN112DATA (Default = ISDN64VOICE)
Answer Tone	Duration of modem answer tone (in 100 ms).	0-50 (in 100 ms) (Default = 36)

Setting up Reserved Modem Pools

EPOS-PAD modems are allocated dynamically as required. An available modem is selected and is then configured for the specified modem class. The threshold setting on the Digital Modem Configuration menu (Figure 17-7) allows a certain number of modems to be reserved for a particular modem class. This is useful, for example, when the total number of modems installed or operating is less than the number of available B-channels. The threshold parameter can also be used to guarantee a certain number of modems for a modem class, to prioritize service for one modem class over another, or to optimize modem use for dial-in calls vs. dial-out calls.

For example, suppose that two modem classes are defined:

- EPOS22 for V.22bis operation
- EPOS32 for V.32 operation.

The threshold for EPOS22 is set to 0. The threshold for EPOS32 is set to 5. This means that no modems are reserved for V.22bis calls: These calls are always in competition for any available modems. However, a minimum of 5 modems are always set aside for V.32 calls. This means that if the number of available modems drops to 5, no V.22bis calls can be established.

Here is an example that maximizes modem use for dial-out calls:

Create a Dial-in modem class and a Dial-out modem class. Set the Dial-in threshold to 119, and the Dial-out threshold to 0. When both modem classes are active, only one modem at most is available for dial-out calls. Dial-in calls can use all 120 modems if necessary.

Unless you intend to restrict service to certain modem classes, it is recommended that the minimum number of guaranteed modems be reserved for a particular class, so that all remaining modems can be allocated dynamically to the different modem classes. This minimizes the possibility of blocked calls for all modem classes.

NOTE: Never set the threshold for a single modem class to the total number of operational modems unless you wish to disable all other modem classes.

Configuring EPOS Profiles

Timer values required by your connection can be specified and stored as a set called an EPOS profile. Up to five EPOS profiles can be created. Once they are created, these profiles are assigned to individual lines as explained in the section *Assigning EPOS-PAD Profile and Modem Class and Adjusting PAD Parameters*.

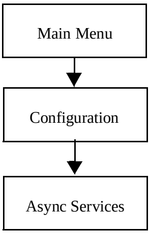
To create an EPOS profile:

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. Select **Async Services**.

✓ The Access Server Commands menu (Figure 17-8) is displayed.




```
*** Access Server Commands ***

1 - PAD configuration options
2 - PAD profiles
3 - X.25 Mnemonics
4 - NUIs
5 - Async services        (PAD, Telnet, IPX-In, SLIP)
6 - Logoff Scripts
7 - EPOS Profiles
8 - Logon Screen          (Initial user screen)
9 - Multicast Configuration

Enter command number:

_________[DynaStar_3df2]__________
Terminate input with <RET>.                Press ESC to return to previous menu.
```

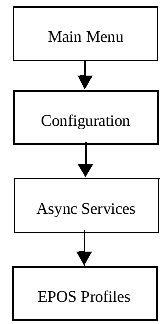
Figure 17-8 Access Server Commands Menu

3. Select EPOS Profiles.

✓ The EPOS Profiles screen (Figure 17-9) is displayed.

4. Change the name of the profile if you wish.

5. If desired, add text in the Optional description field.

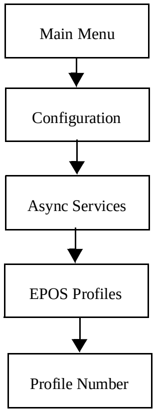



```
                         ***EPOS Profiles***

                                   Last changed: 4-23-02 13:57:55

   Profile name            Optional description
   (1-8 chars)             (up to 32 characters)

1 - EPOS1
2 - EPOS2
3 - EPOS3
4 - EPOS4
5 - EPOS5

          Enter profile number to view/change EPOS parameters:

_______[DynaStar dc000345]_______          Process selections (Y/N): Y
Profile name must not start with number.
Use TAB & CURSOR keys to move among fields.Press ESC to abort command & exit.
```

Figure 17-9 EPOS Profiles Screen

6. In the **Enter profile number...** field at the bottom of the menu, enter the number of the profile you want to configure.

✓ The EPOS Parameter Values screen (Figure 17-10) is displayed.




```
                         ***EPOS Parameter Values***

Profile 1 EPOS1                 Enter value                Permitted values

1:  Ack Timer (Timer A)              6               1-20   seconds
2:  Line Inactivity Timer (Timer C)  60              1-120  seconds
3:  Line Drop Timer                  5               1-20   seconds
4:  X.25 Inactivity Timer            60              1-60   seconds


                                          Process Selections (Y/N):  Y


Press ESC to abort command & exit.            Process selections (Y/N): Y
```

Figure 17-10 EPOS Parameter Menu

7. Set parameters as required. Table 17-2 defines these parameters.

8. When you have completed your configuration, enter **Y** in the Process Selections field and press **<return>**.

✓ You return to the EPOS Profiles screen (Figure 17-9).

9. Repeat steps 4 through 8 for each profile you wish to configure.

10. When you are finished configuring profiles, enter **Y** in the **Process selections field** at the bottom of the EPOS Profiles menu and press **<return>**.

Table 17-2 EPOS Timers

Parameter	Description	Values
Ack Timer (Timer A)	Specifies the time the EPOS PAD waits for an acknowledgment of a data message before retransmitting it.	1-20 seconds (default = 6)
Line Activity Timer (Timer C)	Specifies the time the EPOS PAD waits for a message to be received from the terminal before disconnecting (by sending an X.25 Clear Request and/or a DLE EOT to the terminal).	1-120 seconds (default = 90)
Line Drop Timer	Specifies the amount of time the EPOS PAD waits for an ISDN call to drop after a DLE EOT has been sent to the terminal. When the timer expires, the EPOS PAD drops the ISDN call.	1-20 seconds (default = 5)
X.25 Inactivity Timer	Specifies the time the EPOS PAD waits for a message to be received over the X.25 virtual circuit before disconnecting (by sending an X.25 Clear Request and/or a DLE EOT to the terminal).	1-60 seconds (default = 60)

■ ASSIGNING THE EPOS-PAD PROFILE AND MODEM CLASS AND ADJUSTING PAD PARAMETERS

Modem classes and EPOS profiles are assigned to a particular inbound phone number on the ISDN Incoming Telephone Number menu. You can also adjust port parameters from this menu. To access this menu and make changes:

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu (Figure 3-11) is displayed.

2. Select **Port**.

✓ The Configure Port menu is displayed.

3. Enter the number of the ISDN trunk you want to configure.

✓ The ISDN Port Configuration menu (Figure 17-12) is displayed.

```
***ISDN Port Configuration Menu***

ISDN Interface: Slot 1 E1/PRI2
Type: PRI

1 - Configure PRI/BRI D Channel Port and layer 1 parameters
2 - Configure Incoming Telephone Numbers and SPIDS
3 - Configure B Channel ports

Enter command number:

Terminate input with <RET>.          Press ESC to return to previous menu.
```

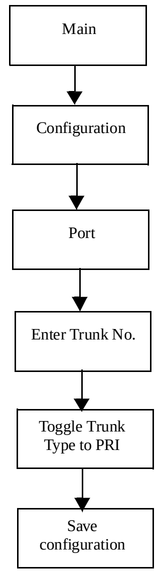
Figure 17-11 ISDN Port Configuration Menu

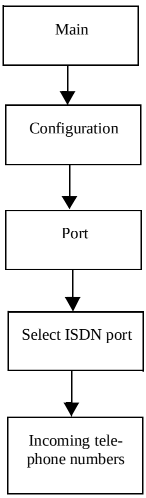
4. Select **Configure Incoming Telephone Numbers and SPIDS**.

✓ The ISDN Incoming Telephone Numbers screen, shown in Figure 17-12, is displayed.

NOTE: Initially, the top telephone number field contains the word DEFAULT. This allows a call from any phone number to be accepted.

You can delete the DEFAULT entry, but if you do and a call is received for a telephone number that is not otherwise defined on this screen, the call is not answered.






```
                    ***ISDN Incoming Telephone Numbers***


ISDN Interface: Slot 1 E1/PRI 2                    Last changed: 4-23-02 13:57:55

     Telephone # (16)   Protocol   Class    SPID (BRI NI-1 & AT&T only) (30)
     -----------------  ------------------------------------------------
01   DEFAULT            PAD        Class 1
02   5553456            PAD        Class 2
03
04
05







_______[DynaStar dc000345]_______          Process incoming numbers (Y/N): Y
To DELETE an entry use <CTRL-D>.To change the protocol or to configure
To view the modem options cursor to the desired entry and enter <CTRL-B>.
PPP/X.25/EPOS PAD options cursor to the desired entry and enter <CTRL-O>.
Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 17-12 ISDN Incoming Telephone Numbers Screen

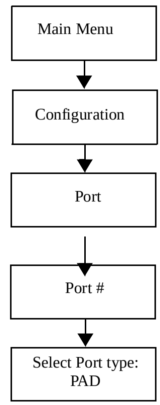
5. Enter a telephone number you expect to receive for EPOS-PAD calls.

6. To configure EPOS parameters, with the cursor on the correct line, enter **<CTRL-O>**.

✓ The Port Configuration menu is displayed.

```
***PAD Port Configuration***
Port 3   IS-232                                   Last changed:  4-23-02  17:00:44

 |---  Press <RET> to toggle values  --| |--- Type in values.  Max chars shown in ()  ---|
Port type:       PAD                  Port name:       Sync/Async                     (14)

                                       Port X.121 address:                      (15 BCD)
                                       X.121 sub-address:                        (2 BCD)
                                       Use sub-address in calling DTE address: N
                                       Inactivity timer: 0          (0-disable, 1-30 min)
Call address field:        None
NUI Required:              N           Enter ? <RET> for profile list
Mnemonic Type:             Normal          X.28 profile: 89   (14)
Port signals option:       TERM            X.29 profile:  00   (00)
Waiting for DSS:           N (fixed)       EPOS profile: 01
Set M-bit on full Pkt:     N           Enter Data Forwarding Char: 00          (00-7F)
Max port forward limit:    NONE        Logoff Script:     0
Autoconnect:               N
Double Break:              N
Drop DSS:                  N           X.28 command:                              (32)
DSS signal:                NORMAL

_______[DynaStar _456d]_______                     Process Selections (Y/N):
Use TAB & CURSOR keys to move among entries. Press ESC to abort command and exit.
```

Figure 17-13 PAD Port Configuration Screen



7. Toggle to select **PAD** as the Port Type and move the cursor to another field (Figure 17-13).

8. Enter the X.121 address of this port.

9. In the EPOS Profile field, enter the number (1-5) of the profile that this PAD port is to use for incoming calls.

   NOTE: When you assign an EPOS profile, the EPOS protocol is enabled for the current telephone number entry.

10. Adjust any other parameters as needed. Table 17-3 lists protocol restrictions that are automatically placed on an EPOS-PAD port and parameters for which specific settings are recommended.

11. When you have completed your changes, move the cursor to the Process Selections field. Enter **Y** and press **<return>**.

✓ You are returned to the ISDN Incoming Telephone Numbers menu.

12. Move the cursor to the Class field and toggle to select the modem class that will be associated with this incoming phone number. (By default, Class1 is assigned.)

NOTE: If NONE is selected in the Class field, no modem is assigned. NONE is intended for use with digitally-based calls and is not currently implemented.

NOTE: You can view (but not change) a Modem class configuration from this screen by entering **<CTRL-B>**. Press **<esc>** to return to the ISDN Incoming Telephone Numbers screen.

NOTE: The SPID field does not apply to EPOS-PAD configuration.

13. When you have configured all phone numbers required, enter **Y** at **Process Incoming Numbers** and press **<return>**.

✓ A message screen (Figure 17-14) is displayed, reminding you that each new phone number must be assigned to a B-channel port.

```
***MESSAGE SCREEN***

A new telephone entry has been defined. It needs to be assigned
to a B channel port before it can be used.

Control will pass to the B Channel port configuration screen so
 that the assignment can be made.

PRESS ESC OR ENTER TO CONTINUE.
```

Figure 17-14 B Channel Configuration Reminder Screen

14. Press **<return>** to continue the configuration process.

✓ The ISDN B Channel Port Configuration screen, as shown in Figure 17-15, appears.

15. Configure the screen as described in the next section.

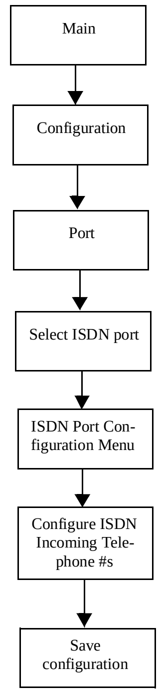
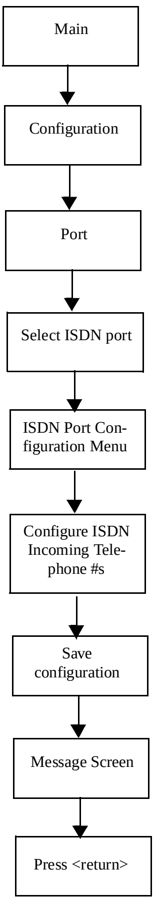


Table 17-3 Required EPOS Port Parameter Settings

Parameter	Setting
Waiting for DSS	Forced to N (fixed)
Call address field	Leave as default (NONE)
NUI required	Leave as default (N)
Mnemonic Type	Leave as default (NORMAL)
Double Break	Leave as default (N)
Enter Data Forwarding Char	Leave as default (No entry)
Logoff Script	Leave as default (0; disabled)
Inactivity Timer	Leave as default (0; disabled)




```
                    ***ISDN B Channel Port Configuration***
ISDN Interface: Slot 1 PRI 1                        Last changed: 4-6-02 13:35:44
   Port   Use        Inbound Tel #     Protocol   ML    Full Time   Config Required
   ------ ---------- ----------------- -------    -     -           -
   101    IN/OUT     DEFAULT           PPP        Y
   102    IN/OUT     DEFAULT           PPP        Y
   103    IN/OUT     DEFAULT           PPP        Y
   104    IN/OUT     DEFAULT           PPP        Y
   105    IN/OUT     DEFAULT           PPP        Y
   106    IN/OUT     DEFAULT           PPP        Y
   107    IN/OUT     DEFAULT           PPP        Y
   108    IN/OUT     DEFAULT           PPP        Y
   109    IN/OUT     DEFAULT           PPP        Y
   110    IN/OUT     DEFAULT           PPP        Y
   111    IN/OUT     DEFAULT           PPP        Y
   112    IN/OUT     DEFAULT           PPP        Y
   113    IN/OUT     DEFAULT           PPP        Y
   114    IN/OUT     DEFAULT           PPP        Y
   115    IN/OUT     DEFAULT           PPP        Y

_______[NetPerformer_dc000345]_______ Process B channel port configuration (Y/N): Y
To DELETE an entry use <CTRL-D>.          To configure port options use <CTRL> O.

Use TAB & CURSOR keys to move among fields. Press ESC to abort command & exit.
```

Figure 17-15 B Channel Port Configuration Screen

Assigning EPOS-PAD Telephone Numbers to B-Channel Ports

Once you have configured new ISDN incoming telephone numbers for EPOS-PAD use as described in the previous section, you must assign each phone number to a specific B-channel port. These assignments are made on the ISDN B-Channel Port Configuration menu (Figure 17-15).

Before you configure this screen, you should be familiar with the contents of the following sections in Chapter 9:

- Directory Number Matching
- B-Channel Assignments and Configuration Order

During the normal configuration process, you are automatically prompted to continue to this screen after setting EPOS-PAD port parameters. If, however, you deferred B-channel assignment or need to modify your entries, access the menu as follows:

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu is displayed.

2. Select **Port**.

✓ The Configure Port menu is displayed.

3. Enter the number of the ISDN trunk you want to configure.

✓ The ISDN Port Configuration menu (Figure 17-12) is displayed.

4. Select **Configure B Channel Ports**.

✓ The ISDN B Channel Port Configuration menu (Figure 17-15) is displayed.

To configure the ISDN B Channel Port Configuration menu:

1. Scroll through the list to select the desired port number.

2. Toggle to select Use as **In** or **In/Out**.

3. Rotate through the available Inbound telephone numbers to select one of those you have configured for an EPOS-PAD connection.

✓ The Protocol field automatically changes to display PAD and the Class field changes to show the Modem class you have configured. The parameters you configured are assigned to the port when a call destined for the inbound phone number is received.

NOTE: The DEFAULT entry in the Inbound Tel # column allows the port to accept calls using any telephone number.

NOTE: Multilink, Full Time, and Additional Configuration options are disabled for EPOS-PAD ports.

4. When you have finished assigning EPOS-PAD numbers to ports, enter **Y** in the Process B channel port configuration field and press **<return>** to save your entries.

✓ You return to the ISDN Port Configuration Menu (Figure 17-11).

ETHERNET SWITCH MODULE

18

■ OVERVIEW

The internal Ethernet switch module can provide up to twelve 10Base-T ports for all *DYNASTAR 100* platforms, the *DYNASTAR 2000/2000H*, and the *DYNASTAR 500*. The *DYNASTAR 2000/2000H* can provide two additional 10/100 Base-T or 10FL/100FX MM/SM ST ports. The module is available in two versions, managed and unmanaged. Different physical modules are used for the two different versions. Interface options include traditional copper, fiber, or a combination of both. Single mode and multi-mode fiber are supported.

The managed version of the module allows the switch to be partitioned into smaller switches and/or to provide additional Ethernet terminal ports that transfer packets internally to the *DYNASTAR* main processor and use the *DYNASTAR*'s routing capability. This allows you to configure different LAN segments within the *DYNASTAR* and route between these LAN's locally or over wide-area networks.

In the unmanaged version, the Ethernet switch is a single standalone module that only takes power from the *DYNASTAR* system. In this version, the ports function as an unmanaged switching hub that simply passes Ethernet packets between ports. By learning which MAC addresses are associated with each port, the switch can optimize packet transfers, thereby improving performance over a non-switching hub. The unmanaged Ethernet switch can link externally to the base 10/100 Ethernet port on the *DYNASTAR* to access the routing and other functions of the *DYNASTAR*.

■ CONNECTIONS

External connections are made to up to six dual RJ-45 10Base-T interface modules on the *DYNASTAR* back panel. Switches on the module provide for crossover so that straight cables can be used for the connections.

If you are connecting with direct fiber connections, one fiber port takes up two physical ports on the *DYNASTAR*. For additional information about fiber connections, see Chapter 19, *Utility Features*.

■ STATUS

Link status is displayed on the front panel LEDs and in the board status screen. On the 500/5000, there is one tricolor LED for each Ethernet port, which displays amber if the link is down and green if the link is up. On the 100/2000, there is one tricolor LED for each Ethernet switch, which displays amber if all links are down and green if any link is up.

■ CONFIGURATION

NOTE: There is no configuration for the unmanaged Ethernet switch module.

The managed Ethernet switch can act as a single network (LAN), or the ports on the switch can be configured as different LANs. These different LANs are also called routing domains. You can then route these LANs internally or externally over a WAN. Configuring the card in this fashion is useful for separating different types of traffic.

There can be any number of LANs/routing domains from 1 to 14. The first 12 ports are 10Mbps ports; ports 13 and 14 can be configured as either 10 or 100Mbps ports.

All ports are assigned a group number, which identifies the routing domain. All ports default to the group number 100 if installed in slot 1 and 200 if installed in slot 2. If the Ethernet switch module is installed in a *DYNASTAR* 5000, the group number will be 300 if the module is in slot 3, 400 if in slot 4, and 500 if in slot 5.

If you want to subdivide the Ethernet switch module to act as separate LANs, then you assign a unique group number to each set of ports in the routing domain.

COMMON PORT CONFIGURATION

The common port (i.e., 100, 200, etc.) is configured first. The individual ports (101-114, 201-214, etc.) are configured after that. The common port configuration governs parameters that apply to all ports 1 through 14 regardless of how many groups/routing domains you configure.

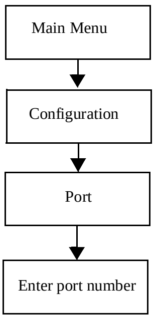
1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu appears.

2. From the Configuration menu, select **Port**.

✓ The Configure Port menu appears.

3. In the **Enter port number** field, enter the group number of the managed Ethernet switch (100, 200, 300, 400, or 500).



✓ The Ethernet Switch Trunk Configuration screen appears (Figure 18-1).

Ethernet switch Trunk configuration

Port: 200 Last Changed: 9-23-02 8:15:59

MAC Address Table: dynamic Ageing Time (sec): 300 RX Buffer Alloc: shared

Port	Group	Speed	Duplex	Flow Ctl	Pri	DLL*	IP	IPX	BRDG	OSI
201	200	10T	half	N	low	N	Y	N	N	N
202	200	10T	half	N	low	N	Y	N	N	N
203	200	10T	half	N	low	N	Y	N	N	N
204	200	10T	half	N	low	N	Y	N	N	N
205	200	10T	half	N	low	N	Y	N	N	N
206	200	10T	half	N	low	N	Y	N	N	N
207	200	10T	half	N	low	N	Y	N	N	N
208	200	10T	half	N	low	N	Y	N	N	N
209	200	10T	half	N	low	N	Y	N	N	N
210	200	10T	half	N	low	N	Y	N	N	N
211	200	10T	half	N	low	N	Y	N	N	N
212	200	10T	half	N	low	N	Y	N	N	N
213	200	10T	half	N	low	N	Y	N	N	N
214	200	10T	half	N	low	N	Y	N	N	N

* Disable TX if RX Link Loss

________[DynaStar_3614]_________ Process selections (Y/N): Y

Use TAB & CURSOR keys to move among fields Press ESC to abort command & exit

Figure 18-1 Ethernet Switch Trunk Configuration Screen

4. Configure the parameters as required. Parameters and values are explained in Table 18-1.

5. When your selections are complete, enter **Y** in the **Process Selections** field and press **<return>.**

Table 18-1 Ethernet Switch Trunk Parameters

Parameter	Description	Values
MAC Address Table	The MAC address of adjacent devices. The Ethernet switch module can learn up to 8000 MAC addresses.	Dynamic (default) Static (not currently available)
Ageing Time	The time, in seconds, after which a MAC address is removed from the table if an idle condition is detected from that device.	10 - 630 secs default = 300 secs

Table 18-1 Ethernet Switch Trunk Parameters (Cont.)

Parameter	Description	Values
RX Buffer Alloc	Receive buffer allocation scheme. Shared shares all of the on-board memory space with all ports. Dedicated assigns each port a fixed number of buffers. If you want to use the built-in flow control mechanism, set this parameter to Dedicated.	Shared (default) Dedicated
Port	The physical *DYNASTAR* port.	x01 - x14, where x = 1, 2, 3, 4, or 5
Group	The logical group number/routing domain identifier. If all ports are to be considered a single LAN, they will all have the same group number. If they are configured as different LAN segments, each LAN will have its own group number.	3-digit number Default= slot number + 00
Speed	The port speed. For ports 1 through 12, the options are 10Base-T (for copper connections) or 10Base-FL (for optical connections). For ports 13 and 14, the options are 10Base-T or 100Base-T (for copper connections), 100Base-FX (for optical connections), or Auto.	10Base-T (default) 10Base-FL 100Base-T 100Base-FX Auto
Duplex	Full or half duplex transmission.	Full Half (default)
Flow Ctl	An internal mechanism that enables the switch to use flow control to slow down attached devices. If Duplex= Half, back pressure is used. If Duplex=Full, IEEE 802.3x flow control is used.To use this option, set RX Buffer Alloc to Dedicated.	Y N (default)

Table 18-1 Ethernet Switch Trunk Parameters (Cont.)

Parameter	Description	Values
Pri	Frames received on ports with high priority are processed internally more frequently than ports set to low priority.	Low (default) High
DLL	Disable Link Loss (applies only to 10Base-T and 10Base-FL ports). Disables the transmitter if the receiver loses the Ethernet link.	Y N (default)
IP	Enables IP traffic for these ports.	Y N (default)
IPX	Enables IPX traffic for these ports.	Not currently supported.
BRDG	Enables bridged traffic for these ports.	Y N (default)
OSI	Enables OSI routing for these ports.	Not currently supported.

IP Configuration

The next step in the configuration is to configure the IP addresses. This can be done in two different ways: either all ports on the module are in a single routing domain, or they are in different routing domains.

Single Domain Configuration. To configure the IP addresses if the Ethernet switch and on-board Ethernet port 0 are seen as a single network (domain):

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu appears.

2. From the Configuration menu, select **Port**.

✓ The Configure Port menu appears.

3. In the **Enter port number** field, enter the group number of the managed Ethernet switch (100, 200, 300, 400, or 500.)

✓ The Ethernet Switch Trunk Configuration screen appears (Figure 18-1).

4. Verify that all ports are assigned to the same group (in this example, 200).

5. Toggle to the first entry in the **IP** column.

6. Press **<return>** to toggle the value from **N** to **Y**.

✓ The IP value for all ports toggles to Y.

7. Enter **Y** in the **Process Selections** field and press **<return>.**

8. Press ESC.

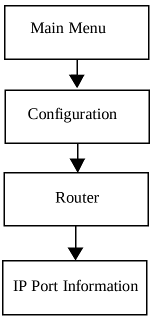
✓ You return to the Configuration Commands menu.

9. From the Configuration Commands menu, select **Router**.

✓ The Router Commands menu appears.

10. From the Router Commands menu, select **IP Port Information**.

✓ The IP Port Information screen appears (Figure 18-2).




```
                        ***IP Port Information***
                                          Last changed: 9-23-02  11:26:45

     Port    Interface        IP Address       IP Mask        |-- Use RET to toggle--|
                                 x.x.x.x          x.x.x.x          Protocol     Encaps
        0     Ethernet          0.0.0.0          0.0.0.0            RIP          Enet II
        3     Sync/Async        0.0.0.0          0.0.0.0            RIP
        4     MODEM 1           0.0.0.0          0.0.0.0            RIP
        5     CSU/DSU chan 2    0.0.0.0          0.0.0.0            RIP
  201-214     Ethernet SW       199.97.53.211    255.255.255.0      RIP
  600-631     Virtual X.25      *

 ________[DynaStar_3614]_________               Process IP addresses (Y/N): Y
Lines with port ranges are multiport interfaces. Configure these ports together on one
line. Or with cursor on line, press <CTRL-O> to configure separately.
*Fields are blank on this screen if ports are configured separately.
```

Figure 18-2 IP Port Information Screen

11. Navigate to the **IP Address** column of the Ethernet switch module ports (201-214 in this example), and enter an IP address for this group. This is the Ethernet network address for this unit. (In this example, the address for Ethernet port 0 in this table remains undefined.)
12. Enter the IP mask in the **IP Mask** column.
13. Enter **Y** in the **Process IP Addresses** field and press **<return>.**

MULTIPLE DOMAIN CONFIGURATION. To configure the addresses if the Ethernet module is to be seen as multiple domains, follow the procedure below. This example partitions the Ethernet switch module into two different domains.

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu appears.

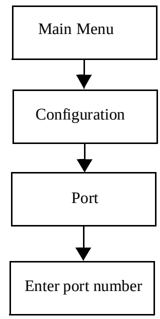
2. From the Configuration menu, select **Port**.

✓ The Configure Port menu appears.

3. In the **Enter port number** field, enter the group number of the managed Ethernet switch (100, 200, 300, 400, or 500.)

✓ The Ethernet Switch Trunk Configuration screen appears (Figure 18-1).

4. Configure the ports into different groups, as required for your network. Figure 18-3 shows an example of the ports divided into two groups (routing domains), 201 and 202.



Ethernet switch Trunk configuration

Port: 200 Last Changed: 9-23-02 8:15:59

MAC Address Table: dynamic Ageing Time (sec): 300 RX Buffer Alloc: shared

Port	Group	Speed	Duplex	Flow Ctl	Pri	DLL*	IP	IPX	BRDG	OSI
201	201	10T	half	N	low	N	Y	N	N	N
202	201	10T	half	N	low	N	Y	N	N	N
203	201	10T	half	N	low	N	Y	N	N	N
204	201	10T	half	N	low	N	Y	N	N	N
205	201	10T	half	N	low	N	Y	N	N	N
206	201	10T	half	N	low	N	Y	N	N	N
207	201	10T	half	N	low	N	Y	N	N	N
208	202	10T	half	N	low	N	Y	N	N	N
209	202	10T	half	N	low	N	Y	N	N	N
210	202	10T	half	N	low	N	Y	N	N	N
211	202	10T	half	N	low	N	Y	N	N	N
212	202	10T	half	N	low	N	Y	N	N	N
213	202	10T	half	N	low	N	Y	N	N	N
214	202	10T	half	N	low	N	Y	N	N	N

* Disable TX if RX Link Loss

________[DynaStar_3614]_________ Process selections (Y/N): Y

Use TAB & CURSOR keys to move among fields Press ESC to abort command & exit

Figure 18-3 Ethernet Switch Trunk Configuration Screen Showing Two Groups

5. Navigate to the first entry in the **IP** column.

6. Press <**return**> to toggle the value from **N** to **Y**.

✓ The IP value for all ports in this group toggles to Y.

7. Navigate to the first entry in the **IP** column for the second group.

8. Press <**return**> to toggle the value from **N** to **Y**.

✓ The IP value for all ports in this group toggles to Y.

9. Enter **Y** in the **Process Selections** field and press **<return>.**

10. Press ESC.

✓ You return to the Configuration Commands menu.

11. From the Configuration Commands menu, select **Router**.

✓ The Router Commands menu appears.

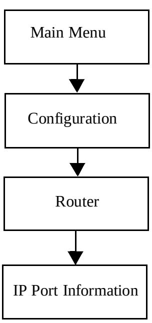
12. From the Router Commands menu, select **IP Port Information**.

✓ The IP Port Information screen appears (Figure 18-2).

13. Assign an IP address and mask to Port 0.

14. Navigate to the Ethernet switch ports (in this example, 201-214) and enter **Ctrl-O**.

✓ The two groups/routing domains that you configured are displayed (Figure 18-4).



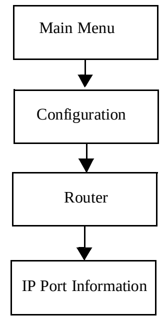

```
                         ***IP Interface (200) Ethernet SW ***
                                        Last changed: 9-23-02  11:26:45

   Port Name or Group     IP Address       IP Mask      |-- Use RET to toggle--|
                            x.x.x.x        x.x.x.x          Protocol    Encaps
Group 201                   5.5.5.5        255.0.0.0        RIP         Enet II
Group 202                   6.6.6.6        255.0.0.0        RIP         Enet II

 ________[DynaStar_3614]_________          Keep new IP addresses (Y/N): Y
You can configure each group as a separate interface.
Press <CTRL-O> to check the corresponding group assignment.
Press ESC to return to the previous screen.
```

Figure 18-4   Group IP Information Screen

15. Enter a unique address and a mask for each group. This will be the address for the *DYNASTAR* on each of these routed LANs.

16. Enter **Y** in the **Keep New IP Addresses** field and press **<return>.**

✓ You return to the IP Port Information screen. It will appear similar to the one shown in Figure 18-5.




```
                          ***IP Port Information***
                                          Last changed: 9-23-02  11:26:45

     Port    Interface         IP Address       IP Mask        |-- Use RET to toggle--|
                                 x.x.x.x         x.x.x.x           Protocol     Encaps
        0      Ethernet          2.2.2.2         0.0.0.0             RIP        Enet II
        3      Sync/Async        0.0.0.0         0.0.0.0             RIP
        4      MODEM 1           0.0.0.0         0.0.0.0             RIP
        5      CSU/DSU chan 2    0.0.0.0         0.0.0.0             RIP
  201-214      Ethernet SW       *
  600-631      Virtual X.25      *

  ________[DynaStar_3614]_________             Process IP addresses (Y/N): Y
 Lines with port ranges are multiport interfaces. Configure these ports together on one
 line. Or with cursor on line, press <CTRL-O> to configure separately.
 *Fields are blank on this screen if ports are configured separately.
```

Figure 18-5   IP Port Information Screen, Multiple Groups

17. Enter **Y** in the **Process IP Addresses** field and press **<return>.**

✓ Your configuration is complete.

UTILITY FEATURES

19

■ OVERVIEW

The *DYNASTAR* includes several features that are specific to the utility industry. These features are described in this chapter and include the following:

- RS-485 interface
- Enhanced environmental specifications
- Fiber optic interfaces
- SCADA bit protocol support
- Direct X.3-FRAD transmission
- Multicast

■ RS-485 INTERFACE

The RS-485 standard permits a balanced transmission line to be shared in a party or multi-drop mode. Up to 32 driver/receiver pairs can share a multi-drop network. The general characteristics of the drivers and receivers are the same as RS-422. The *DYNASTAR* RS-485 interface module can operate in either 2 or 4-wire mode. In 2-wire mode, the transmitter is enabled only when the *DYNASTAR* has data to send and, once complete, the transmitter is tri-stated and the receiver is set to listening mode. In 2- or 4-wire mode, the *DYNASTAR* is generally the Master and all other attached devices are Slaves.

The RS-485 interface can be used on all *DYNASTAR* base HS WAN ports (4 and 5 or 8 and 9) and on the QUAD or 8-port expansion modules. The modules will be detected automatically by the *DYNASTAR* software. Configuration of the 2- or 4-wire mode is set in the Port Configuration menu. The RS-485 module provides an industry standard DB-15 female connector for connection to devices. Pin definitions are given in Appendix B.

The interface module has two sets of jumpers that can be used to provide 120-ohm termination or non-termination of the balanced pair and the ability to provide a DC bias on the transmitter or receive pairs. The bias can provide a forced known idle state for the 2- or 4-wire system when the transmitter or receiver are tri-stated. Default settings are no termination or biasing. See Chapter 2, *DYNASTAR Installation*, for specific jumpering information.

■ ENHANCED ENVIRONMENTAL SPECIFICATIONS

The *DYNASTAR 2000H* is a hardened version of the standard *DYNASTAR 2000* that has been modified to perform, without error or failure, in power utility environments and other hostile industrial environments over and above those covered by the *DYNASTAR* NEBS certification testing.

The modifications include two new power supply options:

- AC/DC 90V-250V
- DC only 20V-60V

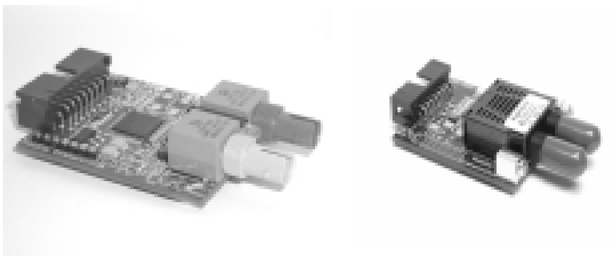
The *DYNASTAR 2000H* was tested to IEEE C37.90.1 Fast Transient, Surge Withstand Capable (SWC) waveforms, 4kV, 2.5kHz. This product is also designed to withstand the Damped Oscillation Waveform test and has successfully passed IEC 61000-4-4 (4kV, 5kHz) and IEC 61000-4-5 (4kV).

The operating temperature of the *DYNASTAR 2000H* has been extended to an operating range of -4° F to +140° F (-20° C to +60° C).

The *DYNASTAR 2000H* is also certified and complies with the new static discharge test defined in the IEEE C37.90.3 specifications. The IEEE adopted the same static standards the NEBS testing required.

■ FIBER OPTIC INTERFACES

The *DYNASTAR* supports fiber optic interfaces (Figure 19-1), as well as standard copper interfaces, directly to various port types (RS-232, T-1, and Ethernet). The modules are available in Multimode (MM) 2 km and Single Mode (SM) 15 km, 40km, and 100km versions. All modules currently adopt the ST mechanical format for the connectors.



For Asynchronous Ports **For T1 or Ethernet Ports**

Figure 19-1 Fiber Optic Interfaces, for Asynchronous Ports (Left) and T1/Ethernet (Right)

NOTE: For asynchronous serial MM and SM connections, as well as 10Base-FL, the fiber interfaces are directly compatible with Dymec links.

Fiber optic modules are available for the following physical interfaces:

- T1/E1 baseWAN ports with integral CSU/DSU
- T1/E1 baseWAN ports with Drop and Insert Master Station Framers
- Asynchronous interfaces on base WAN ports on the *DYNASTAR 100e* and the *DYNASTAR 2000/2000H* models
- Asynchronous interfaces on the QUAD, 8-port, and 16-port expansion modules
- Ethernet Switch expansion module, both managed and unmanaged versions, supporting 10Base-FL 850nm and 100Base-FX 1300nm

NOTE: When replacing copper interfaces with fiber interfaces on the 16-port serial and 12-port Ethernet switch, certain chassis may not allow the full port density to be realized. A single fiber optic module takes up the physical space of two copper ports; therefore, if all optical interfaces are selected, the total port availability will be reduced.

■ SCADA BIT PROTOCOL SUPPORT

The *DYNASTAR* supports the bit-oriented SCADA protocols that are based on a 32-bit message. This differs from traditional asynchronous protocols that use a 10/11-bit format comprising 1 start bit, 8 data bits, and 1 or 2 stop bits. The 32-bit protocols typically consist of one 2-bit sync field, two 12-bit data fields, a 5-bit error checking field, and 1 stop bit. Protocols that comply with the 32-bit format include PMS91 and CONITEL type SCADA messages.

The *DYNASTAR* can transport this type of message on any of the base WAN ports. On the *DYNASTAR 100*, *DYNASTAR 100i*, *DYNASTAR 100e*, and *DYNASTAR 2000/2000H* these are ports 3, 4, and 5. On the *DYNASTAR 500* and *DYNASTAR 5000*, these are ports 7, 8, and 9. The SCADA protocol is also supported on the QUAD serial expansion card. No other serial expansion card can currently support this protocol.

The *DYNASTAR* transports the message by taking the 32-bit word and converting it into four data bytes that are then placed within the payload of a standard frame relay message. At this time, the 32-bit message formats can be transported only over frame relay. At the remote location, the four bytes are converted back into a 32-bit data stream.

For a typical SCADA configuration, see the section *Frame Relay Multicast Configuration* later in this chapter.

■ ASYNC OVER FRAME RELAY SUPPORT (FRAD)

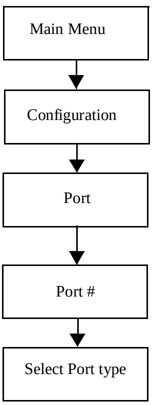
There are a number of ways to transport asynchronous data streams over a Frame Relay network connection. Each method has its own benefits, depending on the application that is running end-to-end. The method most appicable to the utility industry is described below. The other methods are described in Chapter 8, *The Frame Relay Application*.

The X.3-FRAD method simply packages the asynchronous data streams directly into a Frame Relay payload using X.3 protocol. No other protocol is involved. A two-byte frame relay header is pre-pended to the data packets, and they are dispatched. This method uses the least overhead and is therefore very efficient and simple to set up. However, it lacks any method for automatic data recovery in case of errors. This method is usually used in a permanent circuit configuration that does not easily allow alternate routing if the frame relay circuit fails. With this method, the application must compensate for errors in the data, missing packets, and non-responsive devices. The configuration for this method is described below.

X.3-FRAD CONFIGURATION

The port type for all X.3-FRAD connections is PAD; however, not all the PAD parameters are relevant. A typical configuration procedure is given below.

1. From the Main menu, select **Configuration**.
   ✓ The Configuration Commands menu appears.
2. From the Configuration Commands menu, select **Port**.
   ✓ The Configure Port screen appears, with a list of available ports.
3. From the Configure Port menu, enter the number of the port you wish to configure. When the Port Configuration screen appears, toggle the port type to **PAD**.



✓ A Port Configuration screen similar to the one shown in Figure 19-2 appears.

```
                    ***PAD Port Configuration***
Port 3   IS-232                              Last changed:  5-29-02  17:00:44

 |---  Press <RET> to toggle values  --| |--- Type in values.  Max chars shown in ()  ---|
Port type:      PAD              Port name:      sync/async                        (14)

Connection mode:        DCE          Port X.121 address:                      (15 BCD)
Modem speed:            9600 baud    X.121 sub-address:                        (2 BCD)
Parity:                 EVEN         Use sub-address in calling DTE address: N
DSS flow control:       N            Inactivity timer: 0     (0, 1-30 min, 31-255 out)
Call address field:     NONE
NUI Required:           N            Enter ? <RET> for profile list
Mnemonic Type:          NORMAL             X.28 profile: 89   (14)
Port signals option:    TERM               X.29 profile:  00   (00)
Waiting for DSS:        N (fixed)          EPOS profile: 00
Set M-bit on full Pkt:  N            Enter Data Forwarding Char: 00          (00-7F)
Max port forward limit: NONE         Logoff Script:     0
Autoconnect:            N
Double Break:           N
Drop DSS:               N            X.28 command:                               (32)
DSS signal:             NORMAL

_______[DynaStar _456d]_______                   Process Selections (Y/N):
Use TAB & CURSOR keys to move among entries. Press ESC to abort command and exit
```

Figure 19-2 PAD Port Configuration Screen

4. The key parameters for the X.3-FRAD configuration are **Connection Mode**, **Modem Speed**, **Parity**, and **X.28 Profile**. Other parameters may be required depending upon the type of attached devices. Configure parameters as required. All parameters are described in detail in Chapter 7, *The PAD Function*.

   NOTE: In Figure 19-2, parameters that do not apply to the X.3-FRAD application are grayed out.

5. When your configuration is complete, enter **Y** in the **Process selections** field and press **<return>**.

✓ You return to the Configure Port screen.

6. Press **ESC**.

✓ The Configuration Commands menu appears.

7. Select **Frame Relay**.

✓ The Frame Relay Parameters screen () appears.

8. Select **Frame Relay DLCIs**.

✓ The Frame Relay DLCI Configuration Table (Figure 19-3) appears.

9. Toggle the **Type** field to **PAD-FR**.

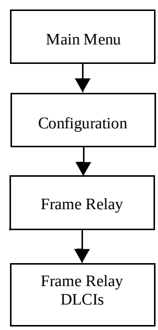
✓ The Source Port is automatically set to the PAD port you configured in the previous steps (port 3 in this example), and a DLCI is assigned.

10. Set the **Destination Port** and **DLCI. Priority**, **CIR**, and **Fragmentation** can be set if required. See Chapter 8, *The Frame Relay Application*, for details.

NOTE: To send the single message from the PAD port to multiple destinations, as in a multi-drop environment, add duplicate entries with the same Source Port and DLCI but with different Destination Ports, as in entries 1 and 2 in Figure 19-3.

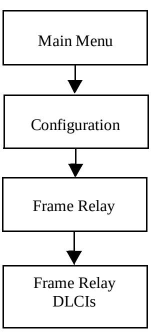
```
                    ***Frame Relay DLCI Configuration Table***
                                             Last changed:  9-23-02  11:26:45

            Source      Dest                                CIR     Fragmnt
  Type      Port  DLCI  Port   DLCI  IP   IPX B  PRTY  Kbps    Bytes      Dest IP Address
1PAD-FR     3     4     100                       1     0       0
2PAD-FR     3     4     101                       1     0       0
3PAD-FR     3     5     100                       1     0       0
4
5
6
7
8
9
10
11
12
13
14
15

 ________[DynaStar_3614]_________             Process selections (Y/N): Y
IUse <CTRl-D> to delete entry              <RET> to toggle or type value
Use <TAB> and CURSOR to move fields        Press ESC to return to previous menu
```

Figure 19-3 Frame Relay DLCI Configuration Table (A)



NOTE: To send the messages received on a DLCI to multiple PAD ports, add an additional PAD-FR entry for each new PAD port. The "original" PAD port must reference all frame relay ports and DLCIs. Subsequent PAD ports need only reference the lowest numbered frame relay port and the lowest numbered DLCI connected to the original PAD port.

Figure 19-4 shows PAD ports 102 and 104 connected to frame relay port 101, DLCIs 100, 200, and 300. Port 102 is the "original" port; therefore, port 104 needs only a one-line configuration (the lowest frame relay port and lowest DLCI). With this configuration, all traffic received on either port 102 or 104 will be sent to port 101, using DLCIs 100, 200, and 300. Conversely, any traffic received on DLCI 100, 200, or 300 will be sent to both ports 102 and 104.




```
                    ***Frame Relay DLCI Configuration Table***
                                           Last changed:  9-23-02  11:26:45

          Source       Dest                                 CIR    Fragmnt
 Type      Port  DLCI  Port   DLCI  IP  IPX  B  PRTY  Kbps   Bytes    Dest IP Address
1PAD-FR   102          101   100                  1     0       0
2PAD-FR   102          101   200                  1     0       0
3PAD-FR   102          101   300                  1     0       0
4PAD-FR   104          101   100                  1     0       0
5
6
7
8
9
10
11
12
13
14
15

 ________[DynaStar_3614]_________               Process selections (Y/N): Y
IUse <CTRl-D> to delete entry                 <RET> to toggle or type value
Use <TAB> and CURSOR to move fields           Press ESC to return to previous menu
```

Figure 19-4 Frame Relay DLCI Configuration Table (B)

11. When your configuration is complete, enter **Y** in the **Process selections** field and press **<return>.**

■ SCADA MULTICAST

The *DYNASTAR* has two multicast functions specifically designed for SCADA applications where a modem multidrop type of environment is replaced by a digital network approach. These are the Frame Relay multicast and the TCP/IP multicast.

In the analog modem environment, the Host port is directly connected to multiple remote IEDs via analog circuits and modems. The analog circuits are physically bridged together and, via RS-485 interfaces, can provide a multi-drop environment where a single host port is fanned out concurrently to multiple remote devices. This is illustrated in Figure 19-5.

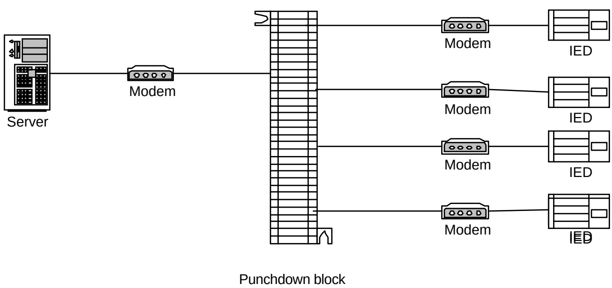


Figure 19-5 Analog Multi-Drop Environment

In a digital or networking approach, the bridged analog circuits are replaced by a gateway product that has a serial connection to the host. The gateway is then connected over a WAN connection to remote IEDs, each IED having its own dedicated connection rather than a shared connection. In this environment, the gateway is responsible for making virtual connections to the remote IEDs (for example, over frame relay). The gateway must multiply or multicast messages received from the host port to each remote device. All remote devices receive the host’s message; however, only the single IED that matches the message address will respond. This response must be routed back over the multicast network and

forwarded to the host. The gateway device is responsible for the message duplication.

SCADA FRAME RELAY MULTICAST

The frame relay multicast function allows an inbound port number and DLCI pair to be defined as the root of the multicast function; a number of outbound port number and DLCI pairs are attached to this inbound stream. The inbound stream can be from a port defined as a frame relay switching port, an Annex G port (X.25 over frame tunnel for carrying synchronous port information), or from a port defined as transparent and carrying MCS-11 or PMS 9 bit-oriented protocol. The Frame Relay Multicast environment is illustrated in Figure 19-6.

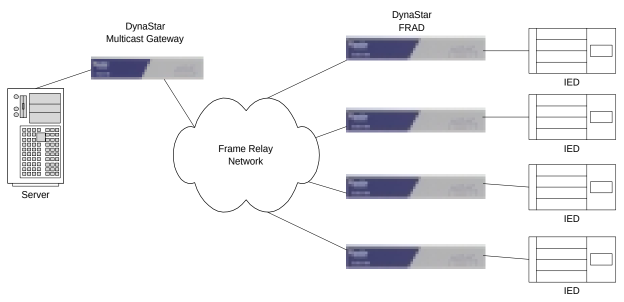


Figure 19-6 Frame Relay Multicast Environment

FRAME RELAY MULTICAST CONFIGURATION. The configuration below gives an example for a PMS-91 setup. This example assumes a primary server on port 3 and a redundant server on port 4.

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu appears.

2. From the Configuration Commands menu, select **Port**.

✓ The Configure Port screen appears with a list of available ports.

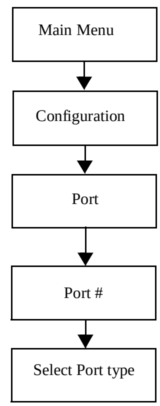
3. From the Configure Port menu, enter the number of the port you wish to configure. When the Port Config-

uration screen appears, toggle the **Port type** field to **Transparent**.

✓ A Port Configuration screen similar to the one shown in Figure 19-7 appears.

```
                    ***Transparent Port Configuration***
Port 3   IS-232                                  Last changed:  5-29-02  17:00:44

 |---  Press <RET> to toggle values  --| |--- Type in values.  Max chars shown in ()  ---|
Port type:       Transparent       Port name:       sync/async                          (14)

Connection mode:          DCE
Line speed:               1200 baud
Protocol:                 SES/PMS-91









_______[DynaStar _456d]_______                        Process Selections (Y/N):
Use TAB & CURSOR keys to move among entries.Press ESC to abort command and exit.
```

Figure 19-7 Transparent Port Configuration Screen



4. Toggle the protocol to **SES/PMS-91**.

✓ The baud rate will automatically change.

5. In the **Process Selections** field, enter **Y <return>**.

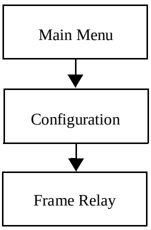
✓ You return to the Configure Port menu.

NOTE: If you have redundant servers, configure a second PMS capable port following steps 1 through 5 above.

6. Press **ESC**.

✓ You return to the Configuration Commands menu.

7. Select **Frame Relay**.



✓ The Frame Relay Parameters menu (Figure 19-8) appears.

```
***Frame Relay Parameters***

1 - Frame Relay DLCIs
2 - FR-ATM DLCIs
3 - Frame Relay Backups/Properties
4 - Frame Relay Priorities

Enter command number:
________[DynaStar_3614]_________
Terminate input with <RET>.            Press ESC to return to previous menu.
```

Figure 19-8 Frame Relay Parameters Menu

8. Select **Frame Relay DLCIs**.

✓ The Frame Relay DLCI Configuration Table (Figure 19-9) appears.

9. In the **Type** column, toggle to select **TRANS-FR**.

✓ The first transparent port (port 3 in this example) automatically appears in the Source Port column. Make sure that the port that is your primary port (if configuring for redundant servers) is the port number that is displayed.

10. Enter the **DLCI** and **Destination Port**.

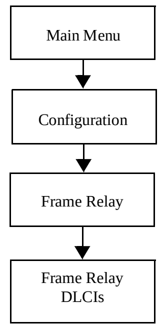
11. To send broadcast messages, duplicate the source port number and map it to a new **DLCI** and/or **Destination Port.** In this example, 10 messages will be broadcast. The DLCI remains the same but the Destination Port changes.

Frame Relay DLCI Configuration Table
Last changed: 9-23-02 11:26:45

Type	Source Port	DLCI	Dest Port	DLCI IP	IPX	B	PRTY	CIR Kbps	Fragmnt Bytes	Dest IP Address
1TRANS-FR	3	5	100				1	0	0	
2TRANS-FR	3	5	101				1	0	0	
3TRANS-FR	3	5	102				1	0	0	
4TRANS-FR	3	5	103				1	0	0	
5TRANS-FR	3	5	104				1	0	0	
6TRANS-FR	3	5	200				1	0	0	
7TRANS-FR	3	5	201				1	0	0	
8TRANS-FR	3	5	202				1	0	0	
9TRANS-FR	3	5	203				1	0	0	
10TRANS-FR	3	5	204				1	0	0	
11TRANS-FR	4	5	100				1	0	0	

________[DynaStar_3614]_________ Process selections (Y/N): Y
Use <CTRl-D> to delete entry <RET> to toggle or type value
Use <TAB> and CURSOR to move fields Press ESC to return to previous menu

Figure 19-9 Frame Relay DLCI Configuration Table, Frame Relay Multicast Configuration



12. To map the same information to the redundant port, select **TRANS-FR** in the **Type** column and toggle until the correct port number appears in the **Source Port** column.

13. Enter the **DLCI** and **Destination Port** for the secondary source port. You need only enter the lowest DLCI and Destination Port for the secondary server; messages to/from the other destination ports will also be sent. Any messages returning on the primary or secondary transparent channels will be sent to both of the PMS ports.

NOTE: The number of broadcast channels available is restricted only by the number of DLCIs available across all Frame Relay applications, which is 1024.

14. **Priority**, **CIR**, and **Fragmentation** can be set if required. See Chapter 8, *The Frame Relay Application*, for details.

15. When you have completed your configuration, enter **Y** in the **Process selections** field and press **<return>**.

SCADA TCP/IP MULTICAST

The TCP/IP multicast feature is similar to the frame relay version. You define a TCP/IP listening IP address and Socket (port) number as the source of the multicast feature. Once the source is defined, you can define a list of destination IP addresses and Socket (port) numbers that are attached to the multicast IP address and socket number. When the source address receives a message, it duplicates the message and forwards it on each of the attached IP address destinations. Messages received from any of the remote IP address destinations are unicast back to the source IP address. The *DYNASTAR* currently supports 16 multicast software elements; up to 16 addresses can be attached to each mulicast element. This is illustrated in Figure 19-10.

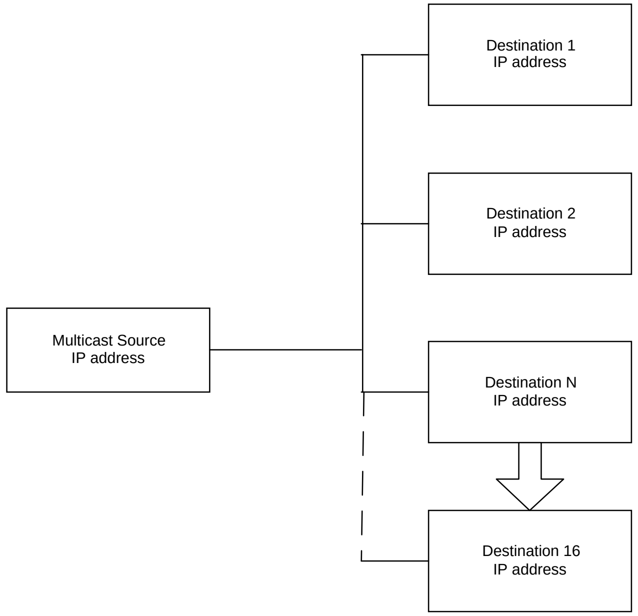


Figure 19-10 Block Diagram of TCP/IP Multicast

The multicast feature can be combined with other software elements to support a number of applications. Examples are given in the sections that follow.

IP APPLICATION. In a pure IP-based system, the Host and IEDs both support IP directly. In this scenario (see Figure 19-11), the Master station simply multicasts the message to remote IP capable devices.

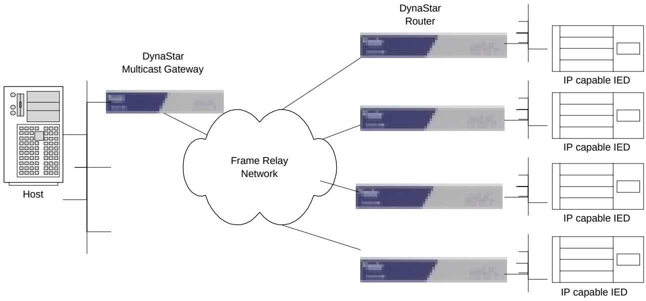


Figure 19-11 IP Multicast Application

ASYNC HOST APPLICATION. In most applications, the Host device generates the SCADA polling over a serial connection. To support this using the IP multicast function, the *DYNASTAR* first converts the serial stream to a TCP/IP stream using the inverse Terminal Server function (X25-IN). (See Chapter 13, *Telnet and Async Services*, for more information on X25-IN.) This application is illustrated in Figure 19-12.

Typically, the serial port can be configured to autocall the X25-In terminal server, which converts the serial data into a TCP/IP format. The Terminal Server then forwards this information to the address defined in the service, which is configured to point to the multicast listening IP address and socket.

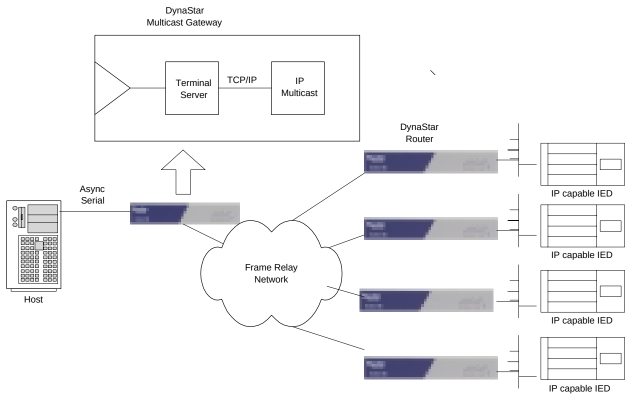


Figure 19-12 Async Host Multicast Application

ASYNC IED APPLICATION. Like most Host applications, most IEDs also communicate over serial ports. Therefore, to use the IP multicast function, they need to employ another software element to convert the TCP/IP multicast connections back to async serial. This feature is available using the terminal server service X25-OutStream (see Chapter 13, *Telnet and Async Services,* for more information on X25-OutStream). This service can be configured to listen to one of the multicast destination IP addresses and sockets and convert the TCP stream back to Async. Figure 19-13 illustrates this application.

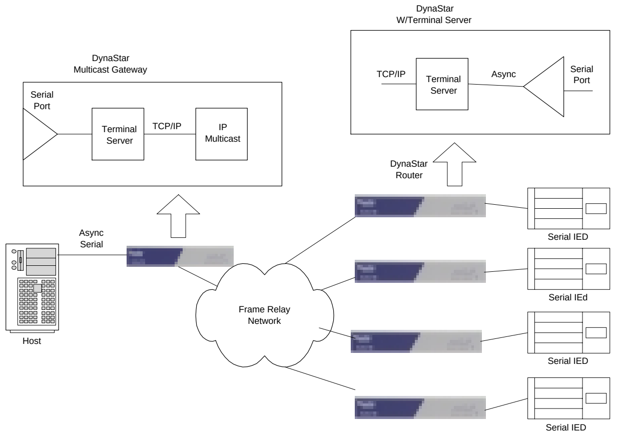


Figure 19-13 Async IED Multicast Application

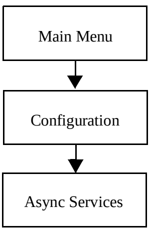
TCP/IP MULTICAST CONFIGURATION. Configure the ports as required by the particular application. (Please refer to the appropriate chapters, as referenced in each application description above.) You configure the multicast software element from the Async Services menu. This is described below.

1. From the Main menu, select **Configuration**.

✓ The Configuration Commands menu appears.

2. From the Configuration Commands menu, select **Async Services**.

✓ The Access Server Commands menu (Figure 19-14) appears.




```
***Access Server Commands***

1 - PAD configuration options
2 - PAD profiles
3 - X.25 Mnemonics
4 - NUIs
5 - Async services                (PAD, Telnet, IPX-In, SLIP)
6 - Logoff Scripts
7 - EPOS Profiles
8 - Logon Screen                  (Initial user screen)
9 - Multicast Configuration

 ________[DynaStar_3614]_________
Terminate input with <RET>.            Press ESC to return to previous menu.
```

Figure 19-14 Access Server Commands Menu

3. Select **Async Services**.

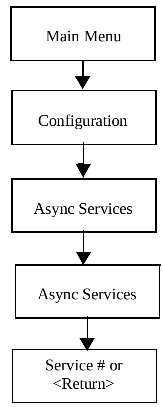
✓ The Async Service Names menu appears.

4. The Async Service Names menu will be blank if no services have been defined. If services have been defined, they will be listed. In either case, press **<return>** to add the new multicast service.

✓ The Async Services screen (Figure 19-15) appears.

```
*** Async Services ***

Service name:          Multicast Test                 (15)
Service type:          Multicast
IP Address             192.100.100.14
Socket Number:         10000
X.121 address:         30077                      (15 BCD)
X.3 Profile:           87 (12) TELNET            (Name or #)
Telnet command:        -E R -D 8                      (23)
CUG:                                                (0-99)
Call UserData:                                        (32)
TCP Idle Timer:        0               (1-255 min., 0=OFF)

_________[DynaStar_3df2]__________          Process selections (Y/N): Y
Use <CTRL-D> to delete entry.            <RET> to toggle or type value
Use TAB & CURSOR keys to move fields.    Press ESC to return to previous menu
```

Figure 19-15 The Async Services Screen



5. Only the first four lines are used for the multicast service. (Lines not needed are grayed out in Figure 19-15.) Enter the information required:

   - **Service name**: A name for this service
   - **Service type**: Toggle for Multicast
   - **IP Address**: Listening or source address
   - **Socket Number**: Listening or source socket

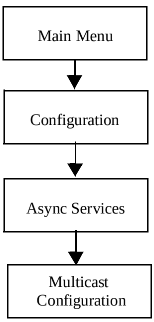
6. When your configuration is complete, enter **Y** in the **Process selections** field and press **<return>.**

✓ You return to the Async Service Names menu. Your new service should now be listed.

7. Press **ESC**.

8. You return to the Access Server Commands menu (Figure 19-14).

9. Select **Multicast Configuration.**



✓ The Multicast Destinations screen appears (Figure 19-16).

```
                    *** Multicast Destinations ***
                                          Last changed: 5-23-02 13:23:55

      IP Address        Socket     Source Socket           Source Name
1     120.1.1.1         1000       10000                   Multicast Test
2     130.1.1.1         1000       10000                   Multicast Test
3     140.1.1.1         1000       10000                   Multicast Test

_________[DynaStar_3df2]__________           Process selections (Y/N): Y
Use <CTRL-D> to delete entry.           <RET> to toggle or type value
Use TAB & CURSOR keys to move fields.   Press ESC to return to previous menu
```

Figure 19-16 Multicast Destinations Screen

10. In the **IP Address** field, define the destination IP addresses.
11. In the **Socket** field, define the destination socket number.
12. In the **Source Socket** field, enter the source port listening socket number that you defined in the Async Services screen above.

    NOTE: You can define up to 16 multicast elements and up to 16 destinations per multicast element.

13. When your configuration is complete, enter **Y** in the **Process selections** field and press **<return>.**

MONITORING AND STATISTICS

20

OVERVIEW

This chapter explains how to obtain certain statistical information about your *DYNASTAR* and the calls that are currently active on your *DYNASTAR* unit. This information can help you locate faults in your system and improve performance. The information in this chapter includes:

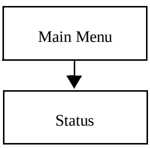
- Obtaining board status information
- Viewing system statistics
- Monitoring physical connections using the built-in data analyzer
- Connection status
- Displaying and clearing the error log
- Obtaining information on buffer usage

BOARD STATUS

The Board Status screen lets you view a list of all ports and board types installed in your *DYNASTAR*. It also tells you what protocol has been configured for each port, whether the port is enabled or disabled, and whether the port is in an up or down state. To access the Board Status screen:

1. From the Main menu, select **Status**.

✓ The Status Commands menu, shown in Figure 20-1, appears.




```
*** Status Commands ***

1 - Board Status          Display internal module types and status
2 - Call status/control   Check call status and manually disconnect calls
3 - Names/Addresses       Verify names & MAC, IP, IPX and X.121 addresses
4 - Statistics            Show statistics for port n
5 - Buffer Usage          System buffer usage
6 - Disable Port          Put port n in Disabled state (busy out dial ports)
7 - Enable Port           Bring port n to an Enabled state
8 - Initialize Port       Perform initialization on port n
9 - Log                   Display system error log
10 - Monitoring           Show input/output data packets for port n
11 - Busy/UnBusy Port     Bring port n to Busy/UnBusy state
12 - PPP status           Check call status
13 - OSI                  OSI operator console
14 - Modem Status         Show statistics & status for modem resources
15 - Call History         Show status of transactions per ISDN port
16 - Trace                SNA Trace

                 Enter command number:

_________[DynaStar_3df2]__________
Terminate input with <RET>.                 Press ESC to return to previous menu.
```

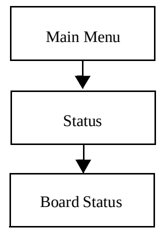
Figure 20-1 Status Commands Menu

2. Select **Board Status**.

✓ The Board Status screen, shown in Figure 20-2, appears. Parameters are explained in Table 20-1.

```
                         *** Board Status ***
DynaStar 100e                                              4-23-02 16:51:55


              Ethernet        SLOT 1           SLOT 2
Port number:  0               101-104          201-214
Name:         Ethernet        IS-QUAD          UnmEtherSW
Interface:    IS-ENET         RS-232           RS-232
Protocol:     ethernet        console          PPP
State:        Enabled         Enabled          Enabled
Status:       Up              Up               Up

              Sync/Async      T1 CSU 1         T1 CSU 2         Console
Port number:  3               4                5                6
Name:         Sync/Async      CSU/DSU chan1    CSU/DSU chan 2   Console
Interface:    RS-232          TDM channel      TDM channel      RS-232
Protocol:     SDLC Host       X.25 line        X.25 line        console
State:        Enabled         Enabled          Enabled          Enabled
Status:       Up              Up               Up               Up - 1
Alarm State:                  No alarms        Yellow alarm
          Enter slot # to view status of multiple-port module:


_________[DynaStar_3df2]__________        Press <RET> for update
                                           Press ESC to return to previous menu.
```

Figure 20-2 Board Status Menu



3. To view information on any expansion boards that have been installed, enter the slot number of the expansion board in the field provided at the bottom of the screen and press **<return>**.

✓ A screen similar to the one shown in Figure 20-3 or Figure 20-4 appears. This screen shows you the port number and electrical interface for the port, the name of the port, the configured protocol, the state, and the status of the port. Figure 20-4 shows the status of T1 trunks for the *DynaStar*. The last port on the trunk status screen is always the D-channel.

Main Menu → Status → Board Status → Enter slot #

*** Alternate Port Status ***

Daughter board ports: Number, Interface, Name, Protocol, State, and Status

101 RS-232	102 RS-232	103 RS-232	104 X.21
QUAD101	QUAD102	QUAD103	QUAD104
HDLC	PPP	PPP	PPP
Enabled	Enabled	Enabled	Enabled
Up	Up	Down	Up

_________[DynaStar_3df2]__________

Press ESC to return to previous menu.

Figure 20-3 Status of Expansion Board Ports

Main → Status → Board Status → Enter Slot #

*** Alternate Port Status ***

Daughter Board ports: Number, Physical level, Protocol type, State, and Status

100	101	102	103	104	105	106	107
T1 trunk	X.25 line	X.25 line	X.25 line	X.25 line	X.25 line	X.25 line	X.25 line
Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
No alarms	Up - 3	Up - 3	Up - 3	Up - 3	Up - 3	Up - 3	Up - 3
108	109	110	111	112	113	114	115
X.25 line	X.25 line	X.25 line	X.25 line	X.25 line	X.25 line	X.25 line	X.25 line
Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
Up - 3	Up - 2	Up - 2	Up -2	Up -2	Down	Down	No alarms
116	117	118	119	120	121	122	123
Zero BW	Zero BW	Zero BW	Zero BW	Zero BW	Zero BW	Zero BW	Zero BW

_________[DynaStar_3df2]__________

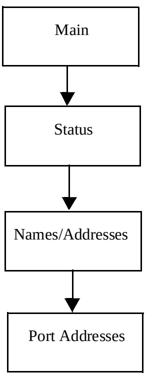
Press <RET> to view more ports.

Figure 20-4 Status Screen Showing T1 Trunks

4. Press **<ESC>** to return to the Board Status menu. You can then request information on another expansion board or return to the Status Commands menu.

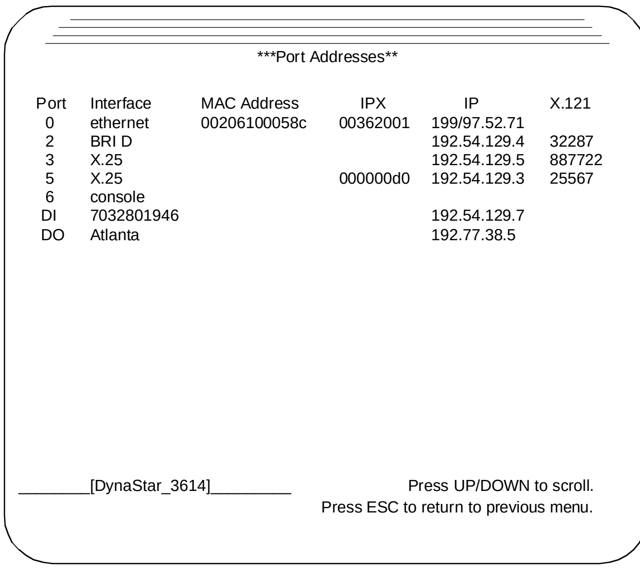
Table 20-1 Board Status Parameters

Parameter	Description
Port number	The number of the port being described. For expansion boards, the slot number is given on the Board Status menu, and the individual port numbers are given on the Alternate Port Status screen.
Name	The name you assigned to this port in the port configuration screen.
Interface	The type of port or type of expansion board installed in the given port or slot number.
Protocol	The type of software interface configured for each installed port. For expansion boards, the interface type is not given on the Board Status menu unless it is identical for all ports on the board. However, the Alternate Port Status screen shows the interface for each individual port.
State	The possible values are Enabled and Disabled. Initially, all ports are enabled.
Status	If a port is disabled, no status is displayed. The possible values are: • UP - *n*, where *n* is the number of active calls on the console,PAD, or X.25 line port. *n* does not appear on the status for any other type of port. • DOWN • Zero BW, (T1 or E1 only) which means no bandwidth has been allocated to this port.
Alarm State	Shows the current state of the CSU physical layer.



■ PORT ADDRESSES

Hardware (MAC), IPX, IP, and X.121 addresses are summarized for all ports on the Port Addresses screen, as shown in Figure 20-5. Note that for ISDN B-Channels, IP and IPX addresses are not always assigned to ports. The IP address is assigned to a PPP Dial Directory entry, an incoming ISDN phone number, or a specific port if it is used for outbound X.25 calls. Therefore, the Port column may indicate DI (dial in), DO (dial out), or a physical port number.



***Port Addresses**

Port	Interface	MAC Address	IPX	IP	X.121
0	ethernet	00206100058c	00362001	199/97.52.71	
2	BRI D			192.54.129.4	32287
3	X.25			192.54.129.5	887722
5	X.25		000000d0	192.54.129.3	25567
6	console				
DI	7032801946			192.54.129.7	
DO	Atlanta			192.77.38.5	

________[DynaStar_3614]_________ Press UP/DOWN to scroll.
Press ESC to return to previous menu.

Figure 20-5 Port Addresses Screen

NOTE: OSPF information is available on special screens. See the section *OSPF Routing* in Chapter 12.

■ PORT STATISTICS

You can use the port statistics screens to monitor traffic statistics and error counts. Statistics are updated every minute as you view the statistics screen; you can also force an update by pressing **<return>**. The specific information that is displayed on the screen will depend on the type of port you are examining.

This section explains how to access the statistics screens and explains all parameters on the screens.

1. From the Main menu, select **Status**.

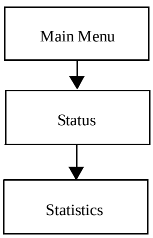
✓ The Status Commands menu, shown in Figure 20-1, appears.

2. Select **Statistics**.

✓ A list of ports on which you can request statistics, similar to the screen in Figure 20-6, appears.

3. From the list of ports, select the port whose statistics you wish to see.

✓ The statistics screen for that port appears. Statistics screens are illustrated in Figure 20-7 through Figure 20-19, and parameters are explained in Table 20-2 through Table 20-10.




```
                              *** Port Statistics ***

Valid port numbers (with names) are:
 0: Ethernet
 6: Console
 7: Sync/Async
 8: HS WAN 1
 9: HS WAN 2
10: Virtual PAD
99: Virtual X.25 Ports

                              Enter port number:

_________[DynaStar_3df2]__________          Press <CTRL-D> to clear all statistics
Terminate input with <RET>.                 Press ESC to return to previous menu.
```

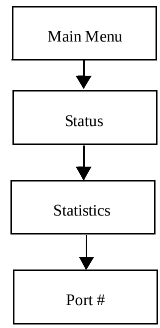
Figure 20-6 Port Statistics Screen

Asynchronous Port Statistics

Asynchronous ports include the PAD, console, IPX-In, IPX-Out, IPX-In/Out, and SLIP ports. Statistics for IPX-In, IPX-Out, IPX-In/Out, and SLIP ports are identical and are shown in Figure 20-7. Parameters are explained in Table 20-2.

The Console and PAD statistics are shown in Figure 20-8 and Figure 20-9, respectively, and parameters are explained in Table 20-3.

Statistics for an asynchronous PPP line are the same as those for a synchronous PPP line and are discussed in the section *Synchronous Port Statistics*.




```
Statistics for Asynchronous port 7:  Async                    Enabled: 6-20-02 17:31:49

Current status:     Down                                      Connection type: Dial (DTE)
Incoming signals:  CD    = Off       CTS = On

                                          To remote      From remote
                           Characters        28               0
                           Frames             0               0
                           ACKs               0               0


Breaks received          =      0
Framing errors           =      0          Parity errors                  =       0
Unrecognized frames      =      0          Async format errors            =       0
Missing frames           =      0          Bad ACKs                       =       0
Frame too long           =      0          Header checksum errors         =       0
Frame checksum errors    =      0          Header type errors             =       0

Overruns                 =      0          Unable to store character      =       0
Timeouts                 =      0          Buffer unavailable             =       0
Transmit failures        =      0          Unable to route to network     =       0

__________[DynaStar_3df2]___________            Press <RET> for statistics update.
Press ESC to return to previous menu.          Press <CTRL-D> to clear statistics.
```

Figure 20-7 Statistics for IPX-In, IPX-Out, IPX-In/Out, and SLIP Ports

Table 20-2 IPX-In, IPX-Out, IPX-In/Out, and SLIP Statistic s

Parameter	Description
Port number	The number of the port whose statistics are being displayed.
Enabled	Date and time the port was enabled.
Current status	Indicates whether a connection is Up or Down.
Connection type	Dial, Leased, or Direct; DCE or DTE electrical interface.
Incoming signals	Status (On/Off) of incoming data set signals.
Characters	The number of characters sent/received.
Frames	The number of IPX-In or SLIP frames sent/received.

Table 20-2 IPX-In, IPX-Out, IPX-In/Out, and SLIP Statistic s(cont.)

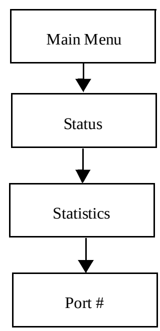
Parameter	Description
ACKs	The number of acknowledgments for IPX-In frames. This figure should match the number of IPX-In frames in the opposite direction.
Breaks received	The number of line breaks (line errors or speed mismatches).
Framing errors	The number of incorrect stop bits on asynchronous character (line errors).
Unrecognized frames	The number of frames that are neither IPX-In frames nor ID strings (IPX protocol errors).
Missing frames	The number of IPX-In frames that are not in sequential order (line errors).
Frame too long	The number of IPX-In or SLIP frames that are too long (IPX or SLIP protocol errors).
Frame checksum errors	The number of IPX-In frames with incorrect checksum (line errors).
Overruns	The number of times that a received character was lost because the RSD register was not empty.
Timeouts	The number of line errors or no responses from the distant end.
Transmit failures	The number of frames not totally transmitted (loss of synchronous clock).
Parity errors	The number of parity errors during modem configuration (modem problems).
Async format errors	The number of IPX-In or SLIP frames that do not begin or end with the proper format characters (line errors).
Bad ACKs	The number of acknowledgments that do not acknowledge current IPX-In frames (delay in remote workstation is greater than the timeout).

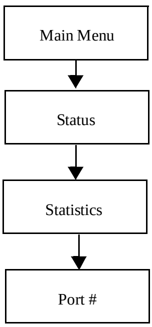
Table 20-2 IPX-In, IPX-Out, IPX-In/Out, and SLIP Statistic s(cont.)

Parameter	Description
Header checksum errors	The number of IPX-In frames with incorrect header checksum (line errors).
Header type errors	The number of incorrect or unrecognized header type field.
Unable to store character	The number of times the system was unable to store a character because the RX buffer was full.
Buffer unavailable	The number of times the system could not transmit because the transmit buffer was full.
Unable to route to network	The number of times the distant network was down or unreachable.

```
Statistics for console port 6:   Console                        Enabled: 4-23-02 17:36:22

Current status:          Up                               Connection type: Direct (DCE)
Flow control status:                                      Incoming signals:
  Received           =  No                                  DTR  =   On
  Sent               =  No                                  RTS  =   On
  Character discard =  0

                To device   From device
Characters       28431       1770                    Parity errors              =     0
Breaks                          0                    Framing errors             =     0
Call attempts        0          3                    Overruns                   =     0
Succeeded            0          2                    Unable to store character  =     0
Failed               0          1

Current call information:                          To net              From net
LCN               = 1              Data packets       41                  195
Call From         =                Data segments      41                  331
    Port          = 6              Data characters    62                  18264
Call To           = 9999           Interrupt packets
    Port          = 19             Reset packets       0                  0
Duration          = 0:05:30

_________[DynaStar_3df2]__________               Press <RET> for statistics update.
Press ESC to return to previous menu.          Press <CTRL-D> to clear statistics.
```

Figure 20-8 Console Statistics with Call Up






```
Statistics for PAD port    101:    PAD2                       Enabled: 4-23-02 17:36:22

Current status:        Down                           Connection type: Direct (DCE)
Flow control status:                                  Incoming signals:
  Received         =  No                                DTR  =   Off
  Sent             =  No                                RTS  =   On
  Character discard = 0

                To device   From device
Characters          0           0          Parity errors               =     0
Breaks                          0          Framing errors              =     0
Call attempts       0           0          Overruns                    =     0
Succeeded           0           0          Unable to store character   =     0
Failed              0           0

_________[DynaStar_3df2]__________           Press <RET> for statistics update.
Press ESC to return to previous menu.      Press <CTRL-D> to clear statistics.
```

Figure 20-9 PAD Statistics with No Call Up

Table 20-3 Console and PAD Statistics

Parameter	Description
Port number	The number of the port whose statistics are being displayed.
Enabled	Date and time the port was enabled.
Current status	Indicates whether a connection is Up or Down.
Connection type	Dial, Leased, or Direct; DCE or DTE electrical interface.
Flow control status	Indicates whether flow control has been sent (Yes/No) or received (Yes/No) and shows the number of characters discarded after flow control is sent. Flow control can be XON/XOFF or data set signals.
Incoming Signals	Status (On/Off) of incoming data set signals.
Characters	The number of asynchronous characters sent/received.

Table 20-3 Console and PAD Statistics (cont.)

Parameter	Description
Breaks	The number of line breaks received.
Call attempts	The number of X.25 calls originated/ received at this port.
Succeeded	The number of successful call attempts.
Failed	The number of failed call attempts.
Parity errors	The number of parity errors (line errors).
Framing errors	The number of incorrect stop bits on asynchronous character (line errors).
Overruns	The number of times that an *Interrupt service routine cannot process character* message has been received from the hardware, indicating there is more traffic than the *DYNASTAR* can handle. Check configuration and verify proper flow control operation.
Unable to store character	The number of times that an *Interrupt service routine cannot store character* message has been received from the hardware, indicating there is more traffic than the *DYNASTAR* can handle. Check configuration and verify proper flow control operation.
Current Call Information	
LCN	The logical channel number of the active virtual call.
Call From/Port	The X.121 address assigned to the local port and the local port's number. The X.121 address is optional and might not be displayed.
Call To/Port	The destination's X.121 address and port in a *DYNASTAR*.
Duration	The call's duration in hours:minutes: seconds.
Data packets	The number of X.25 Data packets sent/received.

Table 20-3 Console and PAD Statistics (cont.)

Parameter	Description
Data segments	The number of accounting data segments sent/received. That is, a Data packet that is 64 bytes or less. A Data packet of 65 bytes counts as two data segments.
Data characters	The number of data characters sent/received in X.25 Data packets.
Interrupt packets	The number of X.25 Interrupt packets sent/received.
Reset packets	The number of X.25 Reset packets sent/received.

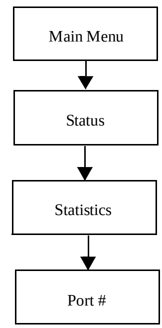
Synchronous Port Statistics

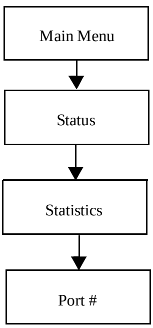
The physical level information for PPP, frame relay, and X.25 port statistics screens is identical and is explained in Table 20-4. The link level information varies among these port types, and only the X.25 port statistics screen includes packet level data. These screens are shown in Figure 20-10 through Figure 20-12. Tables 20-5, 20-6, and 20-7 explain the parameters for the X.25, PPP, and frame relay ports, respectively.

NOTE: Additional statistics are available for PPP. See the section *PPP Protocol Statistics* later in this chapter.

```
Statistics for PPP port      7: PPP1                              Enabled: 4-23-02 17:21:33

Current status:      Up for 0:19:44               Connection type: Dial (DTE)
Incoming signals:  CD =  On   CTS =  On           Last diagnostic code = 160
Physical level:
BadCRCs =     0     FrShort    =      0     FrLong     =     0    Aborts    =       0
Overrun    =     0     Underrun =      0     NoBuffer  =     0    NoRoom=         0
Residue    =     0     TxFrames =      0     RxFrames =     0
Link level:
        To line   From line
UI         0            0          Discarded      =                  0
                                   TxFail         =                  0
                                   RxBadAdd       =                  0

Last Call Information:
Call Direction:      Outgoing                     Telephone Number:     5551300
Call Date:   4/14/97        Call Time:06:04:17
Duration:        0:12:22



__________[DynaStar_730e]_________          Press <CTRL-D> to clear statistics.
Press ESC to return to previous menu.        Press <RET> for statistics update.
```

Figure 20-10 Sample PPP Port Statistics Screen






```
Statistics for frame relay port      3:  FrameRelay1            Enabled: 4-22-02 17:23:07

Current status:     Down                            Connection type: Leased (DTE)
Incoming signals:   CD =  Off   CTS =  On           Last diagnostic code = 160
Physical level:
BadCRCs =     0     FrShort   =       0     FrLong    =      0     Aborts   =            0
Overrun    =  0     Underrun =        0     NoBuffer  =      0     NoRoom=               0
Residue    =  0     TxFrames =        0     RxFrames =       0
Link level:
TxLICS Frames=          0     RxLICS Frames        =      0     RxBadAdd=        0
TxUI Frames    =        0     RxUI Frames          =      0     Discarded=       0
TxFail =                0     Invalid Messages     =      0     Rp/P Timeout=    0

Total DLCIs:            0     Total Active DLCIs          0
Inactive DLCIs:

____________ [DynaStar_44dc]_________            Press <CTRL-D> to clear statistics.
Press ESC to return to previous menu.                Press <RET> for statistics update.
```

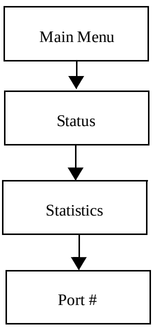
Figure 20-11 Frame Relay Statistics

Table 20-4 Synchronous Port Physical Level Statistics

Parameter	Description
Port number	The number of the port whose statistics are displayed on the screen.
Enabled	Date and time that the port was enabled.
Current status	Indicates whether a connection is Up or Down. Up indicates duration (hh:mm:ss).
Connection type	Dial, Leased or Direct; DCE or DTE electrical interface.
Incoming signals	Status (On/Off) of incoming data set signals.
Last diagnostic code	Reason that the port last changed to Down.
Physical level statistics	
Bad CRCs	The number of frames received with incorrect CRC (or FCS) (line errors).

Table 20-4 Synchronous Port Physical Level Statistics (cont.)

Parameter	Description
Overrun	The number of times that an *Interrupt server routine cannot process a byte* message has been received from hardware, indicating there is more traffic than the *DYNASTAR* can handle. Check configuration for maximum throughput.
Residue	The number of frames received that are not an integral number of octets (protocol error).
FrShort	The number of frames shorter than 4 octets (protocol violation).
Underrun	The number of times that an *Interrupt service routine cannot transfer a byte* message has been received from the hardware, indicating there is more traffic than the *DYNASTAR* can handle. Check configuration for maximum throughput.
TxFrames	The number of physical level frames sent.
FrLong	The number of frames longer than maximum size for type (protocol violation).
NoBuffer	The number of times that an *Interrupt service routine cannot obtain a buffer to store a frame* message has been received, indicating there is more traffic than the *DYNASTAR* can handle. Check configuration for maximum throughput.
RxFrames	The number of physical level frames received.
Aborts	The number of frames aborted by the PDN (line errors).
NoRoom	The number of times that an *Interrupt service routine cannot store a buffer containing a frame* message has been received, indicating there is more traffic than the *DYNASTAR* can handle. Check configuration for maximum throughput.




```
Statistics for X.25 line port        3: X25line                        Enabled: 4-23-02 17:24:45

Current status:      Down                              Connection type: Leased (DTE)
Incoming signals:  CD =  Off   CTS =  On               Last diagnostic code = 160
Physical level:
BadCRCs =     0      FrShort   =       0       FrLong     =      0      Aborts   =          0
Overrun    =    0      Underrun =       0       NoBuffer  =      0      NoRoom=             0
Residue    =    0      TxFrames =      0       RxFrames =      0
Link level:
              To net      From net            To net       From net        To net      From net
SABM          0             0      UA         0               0      RR      0             0
DISC          0             0      I          0               0      RNR     0             0
FRMR          0             0      UI         0               0      REJ     0             0
Discarded=                  0      DM         0               0
T1TimeOt=        0      TxFail =       0       RxPollB =          0      RxBadAdd=          0
Packet level:
                          To net      From net                              To net      From net
Restart                     0            0          Call attempts             0            0
Restart Cause               0            0          Succeeded                 0            0
Restart Confirm             0            0          Failed                    0            0
Reset                       0            0          Reset Cause               0            0
ClearNC =        0      ClearLPE=       0     ClearOCC=      0       ClearDER=          0
Number of Active Calls        0        Max   0              Press <CTRL-D> to clear statistics.
Press ESC to return to previous menu.                         Press <RET> for statistics update.
```

Figure 20-12 X.25 Port Statistics

Table 20-5 X.25 Link and Packet Level Statistics

Parameter	Description
Link level statistics (“to net”=sent; “from net”=received)	
SABM	The number of SABM frames (used to establish the link to the PDN) sent/received.
DISC	The number of DISC frames (used to disconnect the link to the PDN) sent/received.
FRMR	The number of FRMR frames (used to signal protocol violations) sent/received.
Discarded	The number of frames containing LAN traffic that are discarded because too much data is queued for the line (line congestion). This can be remedied by increasing the line speed or limiting the amount of traffic.
T1TimeOt	The number of acknowledgments not received for a SABM, DISC, or Information frame (line error or connection to PDN not available).

Table 20-5 X.25 Link and Packet Level Statistics (cont.)

Parameter	Description
UA	The number of UA frames (unnumbered acknowledgments) sent/received.
I	The number of Information frames (containing X.25 packets) sent/received.
UI	The number of UI frames (unnumbered information) sent/received.
DM	The number of DM frames (used to report that the link is disconnected) sent/received.
TxFail	The number of frames not totally transmitted before the T1 timer expired (loss of synchronous transmit clock).
RxPollB	The number of frames with poll bit set, indicating that the network is performing either error recovery (T1 timeout) or link verification (T3 timeout).
RR	The number of RR (receive ready) acknowledgments to Information frames sent/received.
RNR	The number of RNR frames (used to busy out the link to the PDN) sent/received. A nonzero value indicates congestion.
REJ	The number of Reject frames (used to identify missing Information frames) sent/received.
RxBadAdd	The number of frames received with invalid addresses (X.25 configuration error).
Packet level statistics	
Restart	The number of Restart packets sent/received.
Restart Cause	The cause code for the most recent Restart packet sent/received.
Restart Confirm	The number of Restart Confirmation packets sent/received.
Reset	The number of Reset packets sent/received.

Table 20-5 X.25 Link and Packet Level Statistics (cont.)

Parameter	Description
ClearNC	The number of Clear packets received with clear cause "Network Congestion."
ClearLPE	The number of Clear packets received with clear cause "Local Procedure Error."
Number of Active Calls	The number of X.25 calls currently connected.
Max	High water mark for calls on an X.25 port.
Call attempts	The number of X.25 call attempts sent to and received from the PDN.
Succeeded	The number of successful call attempts sent/received.
Failed	The number of failed call attempts sent/received.
Reset Cause	The cause code for the most recent Reset packet sent/received.
ClearOCC	The number of Clear packets received with clear cause "Line Busy."
ClearDER	The number of Clear packets received with clear cause "Out of Order."

Table 20-6 PPP Link Level and Call Statistics

Parameter	Description
UI	The number of link level UI frames (unnumbered information) sent/received.
Discarded	The number of frames containing LAN traffic that are discarded because too much data is queued for the line (line congestion). Remedy this by increasing the line speed or limiting the amount of traffic.
TxFail	The number of frames not totally transmitted before the T1 timer expired (loss of synchronous transmit clock).

Table 20-6 PPP Link Level and Call Statistics (cont.)

Parameter	Description
RxBadAdd	The number of frames with invalid addresses (protocol violation).
Last Call Information (PRI calls only)	For PPP calls placed over a T1 or E1 Primary Rate Interface, the following information is recorded: call direction (incoming or outgoing), the date and time at which the call was placed, the telephone number called, and the duration of the call (hh:mm:ss).

Table 20-7 Frame Relay Link Level Statistics

Statistic	Meaning
TxLICS Frames	Link management frames transmitted.
TxUI Frames	The number of link level Unnumbered Information frames sent.
TxFail	The number of frames not totally transmitted before the T1 timer expired (loss of synchronous transmit clock).
RxLICS Frames	Link management frames received.
RxUI Frames	The number of link level Unnumbered Information frames received.
Invalid Messages	Invalid link management frames received.
RxBadAdd	The number of frames with invalid addresses (protocol violation).
Discarded	The number of frames containing LAN traffic that are discarded because too much data is queued for the line (line congestion). Either increase the line speed or limit the amount of traffic.
Rp/P Timeout	For the user side, T1 time-out has elapsed without receipt of a STATUS message. For the network side, T2 time-out has elapsed without receipt of a STATUS ENQUIRY message from the subscriber.

Table 20-7 Frame Relay Link Level Statistics (cont.)

Statistic	Meaning
Total DLCIs	The total number of configured DLCIs.
Total Active DLCIs	The number of currently active DLCIs.
Inactive DLCIs	The number of DLCIs currently inactive.

VIRTUAL X.25 PORT STATISTICS

You can gather statistics for virtual X.25 ports just as you would for standard X.25 ports.

1. From the Main menu, select **Status**.

✓ The Status Commands menu (Figure 20-1) appears.

2. From the Status Commands menu, select **Statistics**.

✓ A list of port numbers and names appears

3. Enter **99**.

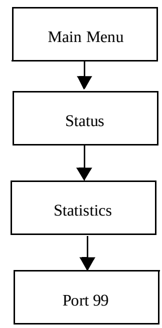
✓ A list of the virtual X.25 ports appears, similar to that shown in Figure 20-13.

```
                         *** Virtual X.25 Ports ***


Valid port numbers (with names) are:
600: V X25 Port 600                 616: V X25 Port 616
601: V X25 Port 601                 617: V X25 Port 617
602: V X25 Port 602                 618: V X25 Port 618
603: V X25 Port 603                 619: V X25 Port 619
604: V X25 Port 604                 620: V X25 Port 620
605: V X25 Port 605                 621: V X25 Port 621
606: V X25 Port 606                 622: V X25 Port 622
607: V X25 Port 607                 623: V X25 Port 623
608: V X25 Port 608                 624: V X25 Port 624
609: V X25 Port 609                 625: V X25 Port 625
610: V X25 Port 610                 626: V X25 Port 626
611: V X25 Port 611                 627: V X25 Port 627
612: V X25 Port 612                 628: V X25 Port 628
613: V X25 Port 613                 629: V X25 Port 629
614: V X25 Port 614                 630: V X25 Port 630
615: V X25 Port 615                 631: V X25 Port 631

              Enter another virtual X.25 port number: 600


_________[DynaStar_730e]__________
Terminate input with <RET>.          Press ESC to return to previous menu.
```

Figure 20-13 Virtual X.25 Ports

4. Enter the number of the virtual port whose statistics you want to view.

✓ A statistics screen similar to the one in Figure 20-14 is displayed. For descriptions of these statistics, see Table 20-5, *X.25 Link and Packet Level Statistics*.

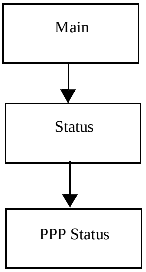


```
Statistics for virtual X.25 port    601: VirtualPort              Enabled: 4-23-02 23:54:13

Current Status: Down                                              Connection type:
Incoming signals:                                                 Last diagnostic code = 0

Link level:                              To net    From net          To net       From net
              To net    From net    I        0          0       UI        0            0
SABM          0          0          RR       0          0       DM        0            0
DISC          0          0          REJ      0          0       FRMR      0            0
UA            0          0          RNR      0          0       Discarded     =        0
T1TimeOt=     0     TxFail =     0          RxPollB =   0       RxBadAdd=  0

Packet level:          To net     From net                     To net         From net
Restart                   0          0          Call attempts       0              0
RestartCause              0          0          Succeeded           0              0
Restart Confirm           0          0          Failed              0              0
Reset                     0          0          Reset Cause         0              0
ClearNC =      0          ClearLPE =      0       ClearOCC =      0   ClearDER=    0
Number of Active Calls      =             0
________[DynaStar_385e________                  Press <CTRL-D> to clear statistics
```

Figure 20-14 Statistics Screen for a Virtual X.25 Port

PPP PROTOCOL STATISTICS

Additional information is available for PPP calls on the PPP Protocol Status Menu (Figure 20-15). Table 20-8 explains this information.




```
                         ***PPP Protocol Status**

                                 Total Frames          Idle Timers (seconds)
Port  IP  IPX   B   COMP   ML   Sent  Recv  Errors      IP     IPX     B
   3   Y   N    N    Y      N   100   120     0        120       0     0
   4   Y   Y    N    N      N   350   347     0         65     120     0
 101   Y   N    N    Y      Y   130   127     0        120       0     0
 103   Y   N    N    Y      Y   120   120     0        120       0     0








 ________[DynaStar_3614]_________
Press <RET> for statistics update.                        Press UP/DOWN to scroll.
Press <CTRL-D> to clear statistics.           Press ESC to return to previous menu.
```

Figure 20-15 PPP Protocol Status Screen

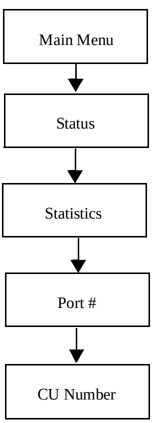
Table 20-8 PPP Protocol Status

Statistic	Meaning
Protocol Status	IP, IPX, Bridged, Compressed, and Multi-link PPP (ML) status. Y indicates the connection can carry this type of traffic. N indicates negotiation has not been completed or has failed, or that this option was not requested in the Dial Directory entry for this connection.
Total Frames	PPP frames sent/received on this connection and number of link level errors.
Idle Timers	The current value of the idle timers that were configured on the Systemwide Parameters screen.

SDLC STATISTICS

Statistics are provided for SDLC terminal and host ports. When you access the statistics screen for an SDLC port, an additional screen appears asking you to provide the CU address of the SDLC device. The statistics screen then appears. The statistics screens for both the terminal and host ports are identical. A sample terminal port screen is shown in Figure 20-16.

The physical level statistics shown in this screen are the same as those given for synchronous ports; they are explained in Table 20-4. The bottom portion of the screen shows how many frames of certain types and Information packets have been sent and received. The left-hand portion of the screen gives statistics for the port, the right-hand portion for the CU.

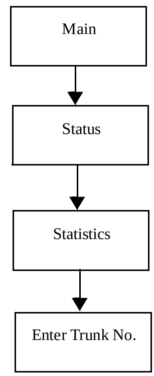



```
Statistics for SDLC Terminal Port 101                       Enabled: 4-23-02 05:45:55
_________[DynaStar_3df2]__________
Current Status:    No alarms                                Connection type:   pt-to-pt
Incoming signals:  CD  =   Off  CTS =  Off

Physical level:                    Bad CRCs        0     Frame too short        0
Frames sent              0         Aborts          0     Frame too long         0
Frames received          0         Overruns        0     No buffers             0
                                   Underruns       0     No room                0
Session Level: CU Poll Address -
Session State:                          Active Connections Thru the Port - 00
                 To Dev     From Dev                          To Dev         From Dev
SNRM               0           0    SNRM                        0               0
DISC               0           0    DISC                        0               0
UA                 0           0    UA                          0               0
DM                 0           0    DM                          0               0
FRMR               0           0    FRMR                        0               0
REJ                0           0    REJ                         0               0
Local Busy         0           0    Local Busy                  0               0
I-Pkts             0           0    I-Pkts                      0               0
Data Bytes         0           0    Data Bytes                  0               0
I-Pkts Lost        0           0    I-Pkts Lost                 0               0
                                                   Press <RET> for statistics update.
Press ESC to return to previous menu.              Press <CTRL-D> to clear statistics
```

Figure 20-16 SNA/SDLC Terminal Port Statistics

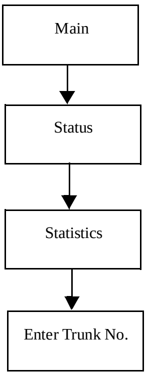
T1/E1 Trunk Statistics

T1 and E1 trunk statistics screens are shown in Figure 20-17 and Figure 20-18, and the fields are explained in Table 20-9. The statistics screens for the individual channels are the same as the statistics screens for any port of that type (frame relay, PPP, or X.25).




```
Statistics for T1 trunk          400                        Enabled: 6-20-02 17:31:49

Current status:                  No alarms

Frame bits in error          =      0
BPV (Line code errors)       =      0
CRC errors received          =      0

Transmitter frame slips      =      0
Tx Elastic Store Full        =      0
Tx Elastic Store Empty       =      0

Receiver frame slips         =      0
Rx Elastic Store Full        =      0
Rx Elastic Store Empty       =      0

Seconds since last error     =      6527




_________[DynaStar_3df2]__________          Press <CTRL-D> to clear statistics.
Press ESC to return to previous menu.        Press <RET> for statistics update.
```

Figure 20-17 T1 Trunk Statistics Screen




```
Statistics for E1 trunk        400                          Enabled: 6-20-02 17:31:49

Current status:                No alarms

Frame bits in error        =      0
BPV (Line code errors)     =      0
CRC errors received        =      0
Far end CRC errors         =      0

Transmitter frame slips    =      0
Tx Elastic Store Full      =      0
Tx Elastic Store Empty     =      0

Receiver frame slips       =      0
Rx Elastic Store Full      =      0
Rx Elastic Store Empty     =      0

Seconds since last error   =      0



__________[DynaStar_3df2]___________          Press <CTRL-D> to clear statistics.
Press ESC to return to previous menu.           Press <RET> for statistics update.
```

Figure 20-18 E1 Trunk Statistics Screen

Table 20-9 T1/E1 Trunk Statistics Parameters

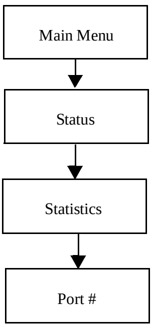
Parameter	Meaning
Enabled	Date and time the port was enabled.
Current status	Indicates whether the trunk has any active alarms.
Frame bits in error	The number of incorrect framing bits.
BPV (Line code errors)	The number of bipolar violations (two pulses of the same polarity in a row).
CRC errors received	The number of CRC errors received on the line.
Far end CRC errors (E1 only)	Number of CRC errors received at the remote end (as indicated by the E-bit setting in frames received from the remote end).

Table 20-9 T1/E1 Trunk Statistics Parameter s(cont.)

Parameter	Meaning
Transmitter frame slips	The number of frame slips (loss of synchronization that caused a bit or bits to be omitted or read twice) on the transmit side. If the number of slips is high, check the configuration of the transmit clock source on the T1 Trunk Parameters screen.
Receiver frame slips	The number of frame slips (loss of synchronization that caused a bit or bits to be omitted or read twice) on the receive side. If the number of slips is high, check the configuration of the transmit clock source on the T1 Trunk Parameters screen.
Tx Elastic Store Full	A transmit slip has occurred because the selected clock is slower than the transmit clock.
Tx Elastic Store Empty	A transmit slip has occurred because the selected clock is faster than the transmit clock.
Rx Elastic Store Full	A receive slip has occurred because the selected clock is slower than the receive clock.
Rx Elastic Store Empty	A receive slip has occurred because the selected clock is faster than the receive clock.
Seconds since last error	The time, in seconds, since the most recent error was reported.

LAN Interface Statistics

The statistics screens for the Ethernet ports provide information on the current operation of these ports. Figure 20-19 illustrates the statistics screen for an Ethernet port. Table 20-10 describes the parameters for Ethernet ports.




```
Statistics for Ethernet port   0:  Ethernet                    Enabled: 4-23-02 16:46:11

Current status:      Up

                                            To LAN        From LAN
                         Frames                407             367
                         Octets              55732           23718
                         Broadcasts              0               0
                         Multicasts              0               0


Frame checksum errors =           0        Transmit not ready      =          0
Receive overflow      =           0        Transmit failure        =          0
Multiple collisions   =           0        Alignment errors        =          0
Too many collisions   =           0        Frame too short         =          0
                                           Frame too long          =          0

                                            OSPF Clock             =          0

__________[DynaStar_3df2]___________          Press <RET> for statistics update.
Press ESC to return to previous menu.        Press <CTRL-D> to clear statistics.
```

Figure 20-19 Ethernet Port Statistics

Table 20-10 Ethernet Statistics

Statistic	Meaning
Port number	The number of the port whose statistics are being displayed.
Enabled	Date and time that the port was enabled.
Current status	Indicates whether a connection is Up or Down.
Frames	The number of LAN frames sent/received.
Octets	The number of octets (bytes) sent/received in LAN frames.
Broadcasts	The number of LAN broadcast frames sent/received.
Multicasts	The number of LAN multicast frames sent/received (not used by IPX).
Frame checksum errors	The number of LAN frames received with incorrect CRCs (LAN transmission errors).

Table 20-10 Ethernet Statistics (cont.)

Statistic	Meaning
Receive overflow	The number of times that more LAN frames were received than the temporary hardware memory buffer (60 kbytes) could store (more LAN traffic than the *DYNASTAR* can process).
Multiple collisions	The number of LAN frames with one or more collisions during transmission (high traffic loads on the LAN).
Too many collisions	The number of LAN frames not successfully transmitted (congestion on the LAN).
Transmit not ready	The number of times the *DYNASTAR* had to wait to transmit a frame (high traffic loads on the LAN).
Transmit failure	The number of times the LAN was not available to transmit a frame (congestion on the LAN).
Alignment errors	The number of LAN frames received that are not an integral number of octets (LAN error condition).
Frame too short	The number of LAN frames received that were less than 64 bytes (LAN error condition).
Frame too long	The number of LAN frames received that were larger than 1514 bytes (LAN error condition).
OSPF Clock	OSPF protocol timeout

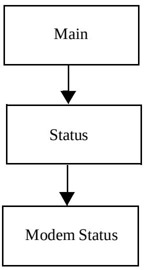
Modem Statistics

General modem status is available for all modems supported by the QPM Module and is provided by modem bank (or slot). Information specific to EPOS-PAD modems is available on an underlying status screen.

General Modem Status. To access general modem status:

1. From the Main menu, select **Status**.

✓ The Status Commands menu(Figure 20-1) is displayed.



2. Select **Modem Status**.

✓ The Modem Status Commands menu (Figure 20-20) is displayed.

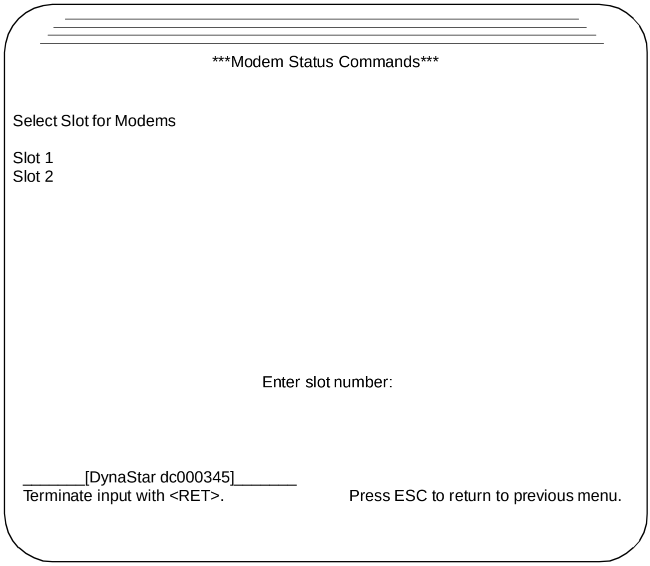


Figure 20-20 Modem Status Commands Screen

3. Select the Slot (Modem Bank) for which you want to display statistics.

✓ The Statistics for Modems screen (Figure 20-21) is displayed. Statistics on this menu are defined in Table 20-11.

```
                    ***Statistics for Modems***
                                     Last Reset: 5-19-02 19:29:50

Current Slot: 2
S   Port   #C   #F  #R  Port   #C   #F  #R  Port   #C   #F  #R  Port   #C   #F  #R
1   209  7297  999   0  OK   7373  999   0  210  7352  999   0  262  7362  999   0
    268  7414  999   0  201  7336  999   0  260  7352  999   0  271  7469  999   0
2    OK  7421  999   0  229  7314  999   0  254  7352  999   0  220  7382  999   0
    256  7364  999   0  265  7360  999   0  251  7352  999   0  258  7418  999   0
3   255  7346  999   0  225  7391  999   0  204  7352  999   0  219  7382  999   0
    206  7399  999   0  257  7384  999   0  228  7352  999   0  264  7275  999   0
4   261  7362  999   0  208  7414  999   0  230  7352  999   0  211  7376  999   0
     OK  7432  999   0  269  7335  999   0  215  7352  999   0  259  7401  999   0
5   ---  ----  ---  --  ---  ----  ---  --  ---  ----  ---  --  ---  ----  ---  --
    ---  ----  ---  --  ---  ----  ---  --  ---  ----  ---  --  ---  ----  ---  --
6   ---  ----  ---  --  ---  ----  ---  --  ---  ----  ---  --  ---  ----  ---  --
    ---  ----  ---  --  ---  ----  ---  --  ---  ----  ---  --  ---  ----  ---  --
7   ---  ----  ---  --  ---  ----  ---  --  ---  ----  ---  --  ---  ----  ---  --
    ---  ----  ---  --  ---  ----  ---  --  ---  ----  ---  --  ---  ----  ---  --


Press <CTRL-A> to clear all Modem statistics   Press <CTRL-N> to view next screen.
Press <CTRL-B> to Busy/Unbusy Modem/Simm       Press <CTRL-D> to clear statistics.
  _______[DynaStar dc000345]_______             Press <RET> for statistics update.
  Press ESC to return to previous menu. Press <CTRL-E> to clear all Modem & PRI
  History statistics.
```

Figure 20-21 General Modem Bank Statistics

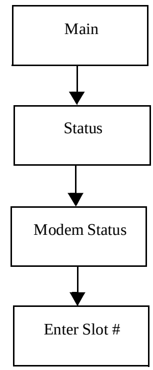


Table 20-11 General Modem Statistics by Slot

Parameter	Description	Values
S	Identifies the octal modem SIMM module.	1 to 8 for banks 2xx 1 to 7 for banks 1xx
Port	Indicates the state of the modem. OK: Ready to be assigned. nnn: Virtual port number to which the modem is allocated. BAD: The modem was taken out of service due to an initialization error. BSY: The modem has been busied out and cannot take calls. ST: The modem is performing a Self-Test. A self test is performed at the completion of each call. ___: The modem was not detected, or diagnostics failed during power up.	Where nnn is 101 to 130 151 to 180 201 to 230 251 to 280
#C	Number of connections (calls) made by this modem.	0-65535
#F	Number of times the modem failed to connect successfully with the remote modem because the physical handshake failed.	0-999 Note: 999 normally indicates an overflow.
#R	Number of times the modem has retrained.	0-999 Note: 999 normally indicates an overflow.

EPOS MODEM STATUS. To access information on EPOS modems supported by the QPM Module:

1. Follow the procedure for accessing General Modem Status in the previous section.

✓ The Statistics for Modems menu (Figure 20-21) is displayed.

2. Press **<CTRL-N>** to access the underlying screen.

✓ The EPOS Modem Statistics menu (Figure 20-22) is displayed. These statistics are defined in Table 20-12.

```
                         ***Statistics for Modems (EPOS)***
                                                Last Reset: 4-3-02 19:29:50

Current Slot: 2
S   Port   #E    #N  #T  Port   #E    #N  #T  Port   #E   #N   #T  Port   #E   #N  #T
1    209  7297  999   0  OK   7373   999  0   210  7352 999   0   262  7362  999   0
     268  7414  999   0  201  7336   999  0   260  7352 999   0   271  7469  999   0
2     OK  7421  999   0  229  7314   999  0   254  7352 999   0   220  7382  999   0
     256  7364  999   0  265  7360   999  0   251  7352 999   0   258  7418  999   0
3    255  7346  999   0  225  7391   999  0   204  7352 999   0   219  7382  999   0
     206  7399  999   0  257  7384   999  0   228  7352 999   0   264  7275  999   0
4    261  7362  999   0  208  7414   999  0   230  7352 999   0   211  7376  999   0
      OK  7432  999   0  269  7335   999  0   215  7352 999   0   259  7401  999   0
5    ---  ----  ---  --  ---  ----   --- --   ---  ---- ---   --   ---  ----  ---  --
     ---  ----  ---  --  ---  ----   --- --   ---  ---- ---   --   ---  ----  ---  --
6    ---  ----  ---  --  ---  ----   --- --   ---  ---- ---   --   ---  ----  ---  --
     ---  ----  ---  --  ---  ----   --- --   ---  ---- ---   --   ---  ----  ---  --
7    ---  ----  ---  --  ---  ----   --- --   ---  ---- ---   --   ---  ----  ---  --
     ---  ----  ---  --  ---  ----   --- --   ---  ---- ---   --   ---  ----  ---  --


Press <CTRL-A> to clear all Modem statistics   Press <CTRL-N> to view next screen.
Press <CTRL-B> to Busy/Unbusy Modem/Simm      Press <CTRL-D> to clear statistics.
  _______[DynaStar dc000345]_______              Press <RET> for statistics update.
  Press ESC to return to previous menu. Press <CTRL-E> to clear all Modem & PRI
  History statistics.
```

Figure 20-22 EPOS Modem Bank Statistics

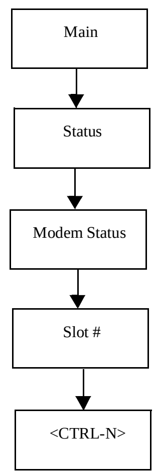
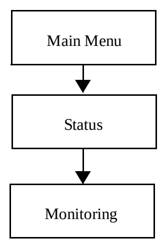


Table 20-12 EPOS Modem Bank Statistic s

Parameter	Description	Values
S	Identifies the octal modem SIMM module.	1 to 8 for banks 2xx 1 to 7 of banks 1xx
Port	Indicates the state of the modem. OK: Ready to be assigned. nnn: Virtual port number to which the modem is allocated. BAD: The modem was taken out of service due to an initialization error. BSY: The modem has been busied out and cannot take calls. ST: The modem is performing a Self-Test. A self test is performed at the completion of each call. ___: The modem was not detected, or diagnostics failed during power up.	Where nnn is 101 to 130 151 to 180 201 to 230 251 to 280
#E	Number of frames received with LRC errors.	0-999
#N	Number of retransmissions due to the receipt of a NAK.	0-999
#T	Number of retransmissions due to a timeout.	0-999

■ MONITORING

The Monitor command provides a live data trace of X.25, frame relay, and Telnet/IP calls, providing you with information on frames and packets sent and received. You can request a limited amount of information (such as link level only or data packets only) and ask that the trace apply only to certain logical channels, DLCIs, or IP addresses and port numbers. By default, all information and the first 100 bytes of data are displayed. The Monitor command can also show you information for other types of calls (such as PPP), but disassembly is not provided.



To use the Monitor command:

1. From the Main menu, select **Status**.

✓ The Status Commands menu (Figure 20-1) is displayed.

2. Select **Monitoring**.

✓ The Monitoring screen, shown in Figure 20-23, is displayed.

```
MOnitor   P;S    Display TX and RX frames for ports
                 P is port #

                 S is any of the following separated by commas:
                 #<lines>          -- maximum lines displayed per packet
                 <chan>—<chan>     -- only selected channels
                 ALL               -- all frames/packets
                 ASCII             -- dump data in ASCII
                 LINK              -- X.25 layer 2 frames
                 PACKET            -- X.25 layer 3 packets
                 DATA              -- X.25 DATA and RR packets/frames
                 NODATA            -- X.25  non-DATA, RR packets/frames
                 TL<socket>        -- Filter on local TCP socket
                 TA<socket>        -- Filter on all TCP traffic on socket
                 IP<IP addr>       -- Filter IP traffic by address
                 IPR<IP addr>      -- Filter received IP traffic by address
                 IPT<IP addr>      -- Filter transmitted IP traffic by address
                 REL or DIFF       -- Display relative or differential time in seconds
                 NONUM             -- Do not display frame numbers
              EX: "MO1;1000" monitor port 1, DLCI 1000

[ESC]         Quit monitor, [CR]          Pause monitor display

ready:
```

Figure 20-23 Monitoring Screen

3. In the **ready:** field at the bottom of the Monitoring screen, enter a monitor command as explained in the next subsection, *The Monitor Command*.

NOTE: To monitor the D-channel on a PRI trunk, use the port number of the trunk itself in the monitor command; for example:
mo 150

✓ For X.25 monitoring, a screen similar to the one in Figure 20-24 appears. For frame relay monitoring, a screen similar to the one in Figure 20-25 appears, and for Ethernet a screen similar to Figure 20-26. The screens show you information on the connections for which you requested monitoring information.

(DTE)		(DCE)		(PORT p ALL LCNs ALL FRAMES)	
XMIT	PF	RCV	PF	Nr Ns Pr Ps LGTH	Hex (20 chars/line)
RR	P			2	0331
		RR	F	2	0331
RR	P			2	0331
		RR	F	2	0331
DISC	P			2	0353
		UA	F	2	0373

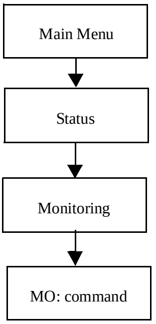


Figure 20-24 X.25 Monitoring Information

XMIT ECN				RCV ECN				(PORT p Frame Relay All DLCIs)	
DLCI	F	B	DE	DLCI	F	B	DE	LGTH	Hex
100	0	0	0					12	184110010B45123498765000
				100	0	0	0	5	184110010F
1023	0	0	1					13	FCF30309007501010103020100
				1023	0	0	0	13	FCF10309007D01010103020101

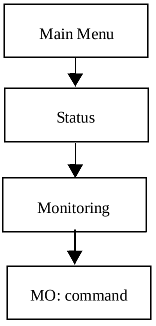
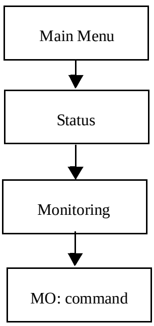


Figure 20-25 Frame Relay Monitoring Information




```
ready:mo0;t23
Destination     Source          Type    Length  Data  PORT 0  Skt 23)
002061003C54    0060975049BD    S         0
0060975049BD    002061003C54    S  A      0
00206100cD54    0060975049BD       A      0
0060975049BD    002061003C54    P  A      6     FFB01FFFD18
002051003C54    0060975049BD    A  0
002061003C54    0060975049BD    P  A      3     FFFD01
006097549BD     002061003C54       A      0
00206100C354    0060975049BD    )  A      3     FFFB18
0060975049BD    002061003C54    P  A      6     FFFA1801FFF0
002061003C54    0060975049BD    P  A      11    FFFA18005654333230FFF0
0060975049BD    002061003C54    P  A      129   0D0A44796E6153746172
                                                5F3631303033633534200
                                                D0A44796E61537461725
                                                F3631303033633534207 3
                                                657276696365730A0A0D
                                                2020202020312020434F4
                                                #534F4C45202020202020
                                                202020202020202020363
                                                . . .
```

Abbreviation	Type	
S	Syn	opening sequence
S A	Syn Ack	
P A	Push Ack	data frame/ acknowledgment
A	Ack	
F A	Fin Ack	closing sequence
R	Reset	

Figure 20-26 Telnet Monitoring Information

4. To pause the information as it scrolls, press **<return>**.

5. When you want to exit from the active monitoring function, press **<ESC>**. However, the trace will continue until the current monitor buffer is dumped.

✓ You return to the Monitoring screen.

THE MONITOR COMMAND. The syntax of the Monitor command is given below:

MO*p*<return>

or

MO*p;parameter,parameter,...*<return>

where *p* is the port number and *parameter* represents any of the items described in Table 20-13 if you are monitoring an X.25 call, Table 20-14 if you are monitoring a frame relay call, and Table 20-15 if you are monitoring other types of calls. For example, the command

MO4;link,002-004<return>

will display link-level traffic on Port 4 for LCNs 2, 3, and 4, and the command

MO4;#5,1022

will display 5 lines of information for DLCI 1022 on port 4.

MO4; TL23

will display Telnet data for IP over X.25 on local socket 23 on port 4.

Table 20-13 X.25 List of Parameters

Parameter	Description
ALL	Display all frames.
LINK	Display only link-level frames.
PACKET	Display only packets.
DATA	Display DATA, RR, RNR, and REJ packets.
NODATA	Display all packets other than DATA, RR, RNR, and REJ packets.
#<lines>	Set the maximum number of lines of a packet to display (from 1-20).
<lcn>	Display packets for this LCN only.
<lcn>–<lcn>	Display packets for the range of LCNs specified (from 0-255).

Table 20-14 Frame Relay Monitoring Parameters

Parameter	Description
<dlci>	Display packets for this dlci only.
#<lines>	Set the maximum number of lines of a packet to display (from 1-20).
<dlci>–<dlci>	Display packets for the range of DLCIs specified (from 16-1023).

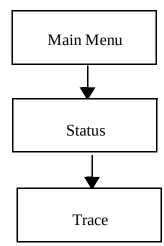
Table 20-15 Additional Monitoring Parameters

Parameter	Description
TL<socket>	Filter TCP/IP traffic based on the local socket number. This allows TCP connections to a particular X.25Out service to be traced.
TA<socket>	Filter on all TCP traffic on this socket number.
IP<IP addr>	Filter IP traffic by the address given.
IPR<IP addr>	Filter received IP traffic for the address given.
IPT<IP addr>	Filter transmitted IP traffic for the address given.
REL or DIFF	Display relative or differential time in seconds.
NONUM	Do not display frame numbers.

■ THE SNA TRACE FUNCTION

The DLC-XPAD and DLC-FRAD provide a data monitor function for both SDLC and LLC traffic over the X.25 or frame relay connections.

To activate the SNA trace on a per-port basis:



1. From the Main menu, select **Status**.

✓ The Status Commands menu appears (Figure 20-1).

2. From the Status Commands menu, select **Trace**.

✓ The Trace menu, shown in Figure 20-27, appears and displays the *DYNASTAR* ports.

```
                              *** Trace Menu ***
 Port Names                                    Port Interface Type

   0: Ethernet            N                    ethernet
   3: Sync/Async          N                    SDLC Term
   4: CSU/DSU chan 1      N                    X.25 line
   5: CSU/DSU chan 2      N                    X.25 line
   6: Console             N                    console
 101: QUAD101             N                    X.25 line
 102: QUAD102             N                    PPP
 103: QUAD103             N                    PPP
 104:QUAD104              N                    PPP



 Press <RET> to toggle values


_________[DynaStar_3df2]__________                       Start trace (Y/N): N
Press any key to stop trace.
Use TAB & CURSOR keys to move among fields. Press ESC to return to previous menu.
```

Figure 20-27 Trace Menu

3. Choose the port(s) that you want to monitor by toggling to select **Y** in the column following the port number and name.

NOTE: A trace can be activated only on SDLC, X.25, and frame relay ports.

4. To activate the trace, enter **Y** in the **Start trace** field at the bottom of the menu and press **<return>**.

✓ As soon as the trace is activated, trace information appears on the supervisory console for all selected ports. SDLC trace information is similar to that shown in Figure 20-28; X.25 (LLC) trace information is similar to that shown in Figure 20-29; and frame relay port trace information is similar to that shown in Figure 20-30. The trace information is explained in Tables 20-16 through 20-18.

NOTE: If the trace facility encounters difficulty decoding a frame, it outputs the message *SDLC frame could not be decoded* or *LLC frame could not be decoded,* as appropriate.

5. To stop the trace, press **<ESC>**.

✓ You return to the Trace menu.

Table 20-16 SDLC Trace Information

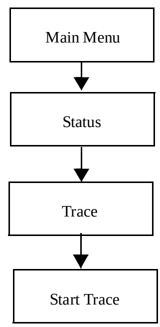
Field Name	Description
Portnum	Port number.
CU address	CU poll address.
Rx or Tx	Direction of traffic. Rx=frame received by the port. Tx=frame originated by the port.
RR, DM, etc.	Type of frame.
NS or NR	Sequence number of the next frame to be sent (NS) or to be received (NR).
CTRL	The SDLC control field.
Data Size=‘Data Length’	The length of the following field.
Data=‘SNAdata’	The first 32 bytes of an I-frame/XID frame.
ticks=n...n	Time stamp in 250 msec increments.

```
portnum = 3 CU = 01 Rx RR NR = 06 CTRL = 01 ticks =    17105

portnum = 3 CU = 01 Tx RR NR = 06 CTRL = 01 ticks =    17105
```

Figure 20-28 Typical Trace Display for SDLC Ports

```
Portnum = 5  GFI = 10 LCN = 10 TxDATAPKT DSAP = 02  SSAP = 04  Data Size = 128

Data = 11 14 3A 3A 3A ............2A

ticks = 44597
```

Figure 20-29 Typical Trace Display for SNA over X.25




```
portnum = 4 DLCI = 0x064, L2 = 4c 80 L3 = 70 82 DSAP = 40 SSAP = 40 Tx RR NR =0

6 CTRL = 01 CR = 00 PF = 01 ticks =    17106

portnum = 4 DLCI = 0x064, L2 = 4c 80 L3 = 70 82 DSAP = 40 SSAP = 40 Rx RR NR =0

6 CTRL = 01 CR = 01 PF = 01 ticks =    17108
```

Figure 20-30 Typical Trace Display for Frame Relay Ports

Table 20-17 SNA over X.25 Trace Information

Field Name	Description
Portnum	Port number.
GFI	10 (=Modulo 8).
LCN=	Logical channel number in hex.
Rx or Tx	Direction of packet. Rx=received by the port. Tx=originated by the port.
‘packet Type’	Type of packet, such as RRPKT, CALL-PKT, ACCEPTPKT, DATAPKT, CLEAR-PKT.
Diag	Value of diagnostic code in Clear packets.
DSAP	Destination Service Access Point. The first byte of the LLC2 header in the X.25 Data packet payload field (if present).
SSAP	Source Service Access Point. The second byte of the LLC2 header in the X.25 Data packet payload field (if present).
Data Size	The length of the X.25Data packet payload field.
Data=‘SNAdata’	The first 32 bytes of the payload field of X.25 Data packets excluding DSAP, SSAP, and LLC control fields.
Ticks ‘n...n’	Timestamp in 250msec increments.

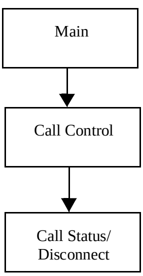
Table 20-18 SNA over Frame Relay Trace Information

Field Name	Description
Portnum	Port number.
DLCI	DLCI number.
L2	RFC 1490 layer 2 field indicating LLC2.
L3	RFC 1490 layer 3 field indicating non-Appn SNA peripheral traffic. This is the only encoding supported.
DSAP	Destination Service Access Point. The first byte of the LLC2 header.
SSAP	Source Service Access Point. The second byte of the LLC2 header.
RX or TX	Direction of frame. RX = Receive by the port. TX = Originated by the port.
Type	Type of frame. (DM, RR, etc.)
CTRL	The value of the Control field. The third byte of the LLC2 header.
CR	The value of the C/R (Command/Response) bit as indicated by the control field or subcontrol field for an Information, Supervisory, or Unnumbered frame.
PF = ‘ ’	The Poll/Final bit value as indicated by the control field or subcontrol field for an Information, Supervisory, or Unnumbered frame.
Data Length	The length of the following field.
SNA Data	The first 32 bytes of the protocol data unit.
Ticks = n...n	Time stamp in 250 msec. increments.

■ MONITORING DIAL CALLS

Use the Call Status/Disconnect screen (Figure 20-31) to monitor dial ports configured on ISDN B-channels when the connection mode is set to **On Demand**. WAN ports also appear on this screen when they are configured for PPP operation and the connection mode is **Dial**.

The Call Status/Disconnect screen is updated automatically every 60 seconds or each time you press **<return>**.
To reset all statistic counters to zero, type **<CTRL-D>**.
Table 20-19 describes Call Status parameters. Table 20-20 provides definitions for Clear Causes.




```
                         ***Call Status/Disconnect**

                                                          Last
                                                  Call    Call duration   Clear
Port   Interface    Type  Called number   Progress   dd/hh/mm/ss     Cause
  3    B Channel 2   PPP   7035553007    Connected  00:13:45
  4    B Channel 1   PPP   7035553007    Idle       00:02:13        -16
101    B Channel 7   PPP   7035553009    Connected  00:07:14



                 To disconnect a call, enter port number:

 ________[DynaStar_3614]_________
Press <RET> for statistics update.                    Press UP/DOWN to scroll.
Press <CTRL-D> to clear statistics.          Press ESC to return to previous menu.
```

Figure 20-31 ISDN Call Status/Disconnect Screen

Table 20-19 Call Status/Disconnect Parameters

Parameter	Description
Port	*DYNASTAR* port number.
Interface	B-channel for an ISDN port; RS-232 or V.35 for a WAN port.
Type	The type of traffic the port is configured to handle.
Called number	For this *DYNASTAR*, called location. For incoming calls, phone number or ID of the originator when permitted.
Call Progress	Idle, calling, or connected.
Call duration	Length of calls in days:hours:minutes:seconds.
Last Clear Cause	Reason last call was cleared. See Table 20-20 for definitions.

Table 20-20 indicates the reason for ISDN call clearing, failure, or completion. Call failures are indicated in the Clear Cause field on the ISDN Call Status/Disconnect menu (Figure 20-31).

Table 20-20 ISDN Cause Code s

Cause Code	Description
1	Unallocated (unassigned) number
2	No route to specified transit network
3	No route to destination
6	Channel unacceptable
7	Call awarded and being delivered in an established channel
16	Normal call clearing
17	User busy
18	No user responding
19	No answer from user (user alerted)
21	Call rejected
22	Number changed
26	Nonselected user clearing
27	Destination out of order
28	Invalid number format
29	Facility rejected
30	Response to status enquiry
31	Normal, unspecified
34	No circuit/channel available
38	Network out of order
41	Temporary failure
42	Switching equipment congestion
43	Access information discarded

Table 20-20 ISDN Cause Codes (cont.)

Cause Code	Description
44	Requested circuit/channel not available
47	Resources unavailable, unspecified
49	Quality of service unavailable
50	Requested facility not subscribed
57	Bearer capability not authorized
58	Bearer capability not presently available
63	Service or option not available, unspecified
65	Bearer capability not implemented
66	Channel type not implemented
69	Requested facility not implemented
70	Only restricted digital information bearer capability is available
79	Service or option not implemented, unspecified
81	Invalid call reference value
82	Identified channel does not exist
83	A suspended call exists, but this call identity does not
84	Call identity in use
85	No call suspended
86	Call having the requested call identity has been cleared
88	Incompatible destination
91	Invalid transit network selection
95	Invalid message, unspecified
96	Mandatory information element is missing
97	Message type nonexistent or not implemented
98	Message not compatible with call state or message type non-existent or not implemented

Table 20-20 ISDN Cause Codes (cont.)

Cause Code	Description
99	Information element nonexistent or not implemented
100	Invalid information element contents
101	Message not compatible with call state
102	Recovery on timer expiry
111	Protocol error, unspecified
127	Interworking, unspecified

■ ISDN CALL HISTORY

The ISDN PRI Call History menu groups summary information for an entire ISDN module and provides access to underlying screens that contain statistics on modem types and X.25 line performance.

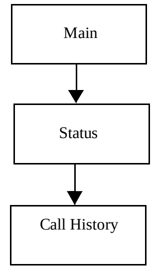
To view a summary of PRI calls:

1. From the Main menu, select **Status**.

✓ The Status Commands menu is displayed.

2. Select **Call History**.

✓ The ISDN PRI Call History menu (Figure 20-32) is displayed. The statistics displayed are defined in Table 20-21. Table 20-22 defines the protocol codes that can appear on this screen. You can view the two underlying screens (Figure 20-33 and Figure 20-34) and then return to this screen by pressing **<CTRL-N>** repeatedly.




```
***ISDN PRI Call History***
                                        Last Reset: 5-16-02 19:29:50

Current Slot 1 & 2
Active Channels
Port      State channel            1 1 1 1 1 1 1 1 1 1  2 2 2 2 2 2 2 2 2 2 3 3
                  1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Trunk 1/1 OK  _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Trunk 1/2 OK  _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Trunk 2/1 OK  _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Trunk 2/2 OK  _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

History         Trunk 1/1   Trunk 1/2   Trunk 2/1   Trunk 2/2   Total
# ISDN call    :    0           0          10          10        20
# Total succ.  :    0           0          10          10         0
# Port unav    :    0           0           0           0         0
# Modem unav   :    0           0           0           0         0
# ISDN fail    :    0           0           0           0         0
# Handskfail   :    0           0           0           0         0
# Neg fail     :    0           0           0           0         0


 Press <CTRL-B> to Busy/Unbusy Trunk
 Press <CTRL-A> to clear all statistics        Press <CTRL-N> for next screen.
 _______[DynaStar dc000345]_______             Press <RET> for statistics update.
  Press <ESC> to return to previous menu.      Press <CTRL-D> to clear statistics.
```

Figure 20-32 PRI Call History Screen

Table 20-21 PRI Call History Status Parameters

Parameter	Meaning	Value
Port	The name assigned to the primary link.	14 chars Default= Trunk 1/1, etc.
State	OK: calls can be accepted on the link. Busy: No new calls accepted; calls in progress will be allowed to complete. A trunk that is OK displays the state of each transaction on each of its B-channels. A busy trunk does not show any information once the B-channels are closed.	OK or BSY
x	Protocol running on the B-channel	See Table 20-22 for possible values.

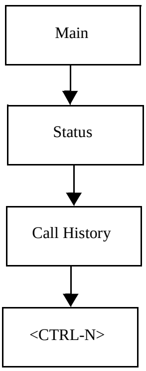
Table 20-21 PRI Call History Status Parameter s(cont.)

Parameter	Meaning	Value
# ISDN call	The total number of ISDN calls received on that trunk. (These calls may or may not have been accepted.)	0 to 999999
# Total succ	The total number of successful transactions on that trunk.	0 to 999999
# Port unav	The total number of calls rejected because a B-channel port was not available.	0 to 999999
# Modem unav	The total number of calls rejected because a modem was not available.	0 to 999999
# ISDN fail	The total number of calls rejected by ISDN for reasons other than Port failure or Modem failure (for example, unsupported rate indicated in bearer capabilities information element of an incoming Setup packet).	0 to 999999
Handsk fail	The total number of calls cleared because the modem's physical handshake failed.	0 to 999999
Neg fail	The total number of calls cleared because the configured error correction/data compression protocol could not be negotiated.	0 to 999999

Table 20-22 B-Channel Protocols

Protocol	Code
Idle	-
Async PPP	P
Sync PPP	S
PAD	A
X.25	X
EPOS	E
SLIP	L
Frame Relay	F

MODEM STATISTICS. An ISDN modem statistics menu (Figure 20-33) provides information on the total number of connections for various types of modems, as well as the number of connections for each trunk. To view these statistics, press CTRL-N from the ISDN PRI Call History screen.



*** ISDN PRI Call History (Modems) ***

Last Reset: 4-23-02 19:29:50

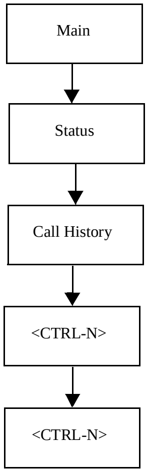
History	Trunk 1/1	Trunk 1/2	Trunk 2/1	Trunk 2/2	Total
# V.34 :	0	0	34	15	59
# V.32bis :	0	0	0	0	0
# V.32 :	0	0	10	81	91
# V.22bis :	0	0	0	0	0
# V.22 :	0	0	0	0	0
# V.21 :	0	0	0	0	0

Press <CTRL-A> to clear all statistics
_______[DynaStar dc000345]_______
Press ESC to return to previous menu.

Press <CTRL-N> for next screen.
Press <RET> for statistics update.
Press <CTRL-D> to clear statistics.

Figure 20-33 ISDN PRI Call History Screen for Modems

EPOS-PAD CALL HISTORY. You can view summary statistics for all EPOS-PADs connected to an ISDN PRI (Figure 20-34) by pressing CTRL-N from the PRI Call History (Modems) screen. Table 20-23 defines the statistics displayed.




```
                    ***ISDN PRI Call History (EPOS)***
                                        Last Reset: 4-23-02 19:29:50

History        Trunk 1/1    Trunk 1/2    Trunk 2/1    Trunk 2/2    Total

# Rx A Nua      :    0          0           10          81          91
# Tx ENQ        :    0          0            0           0           0
# Rx DLE EOT    :    0          0           34          15          59
# Tx DLE EOT    :    0          0            0           0           0
# ISDN T.O.     :    0          0            0           0           0
# X.25 T.O.     :    0          0            0           0           0
# Unexptd Clr   :    0          0            0           0           0
# LRC errors    :    0          0            0           0           0
# Re Tx Nak     :    0          0            0           0           0
# Re Tx TO      :    0          0            0           0           0
# Unexpd Disc   :    0          0            0           0           0


Elapse time per successful transaction:            Min: 00   Max: 0    Avg: 0 (s)
Max number of simultaneous transactions:           Min:      at: 7-2-98  15:36:22

 Press <CTRL-A> to clear all statistics       Press <CTRL-N> for next screen.
 _______[DynaStar dc000345]_______             Press <RET> for statistics update.
  Press ESC to return to previous menu.         Press <CTRL-D> to clear statistics.
```

Figure 20-34 ISDN PRI Call History Screen for X.25 Protocol

Table 20-23 EPOS-PAD-Specific Call History

Field	Description	Value
# Rx A Nua	Total number of A Nuas received	0 to 999999
# Tx ENQ	Total number of ENQs transmitted	0 to 999999
# Rx DLE EOT	Total number of DLE EOTs received	0 to 999999
# Tx DLE EOT	Total number of DLE EOTs transmitted	0 to 999999
# ISDN T.O.	Total number of ISDN inactivity timeouts	0 to 999999
# X25 T.O.	Total number of X.25 inactivity timeouts	0 to 999999
# Unexptd Clr	Total number of unexpected X.25 Clear Requests	0 to 999999

Table 20-23 EPOS-PAD-Specific Call History (cont.)

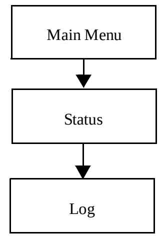
Field	Description	Value
# LRC errors	Total number of frames received with LRC error	0 to 999999
# Re Tx Nak	Number of NAKs received from remote EPOS device	0 to 999999
# Re Tx T.O.	Total number of incomplete frames received following a transmission timeout	0 to 999999
# Unexpected Disc.	Total number of unexpected ISDN call terminations without either party having sent a DLE EOT sequence	0 to 999999
Elapsed time per successful transaction (Min., Max., Avg.)	Minimum, maximum, and average Time required for successfully completed transactions	0 to 999999
Max number of simultaneous transactions	Maximum number of simultaneous transactions recorded during this sampling period	0 to 999999

■ System Log

The system log records:

- The reason a port goes to down status
- Problems with dial modems
- Availability of the file server
- Software integrity errors
- System reset reasons

The Log menu lets you view the system log. The log is displayed in the order in which the messages were generated, regardless of their severity. Figure 20-35 shows a sample System Error Log.




```
System error log:


10/2/97 16:45:37   Configuration file empty
10/2/97 16:45:37   Configuration file initialized to default values
10/2/97 16:45:37   ROM version 3.9
10/2/97 16:45:37   Serial number 3df2
10/2/97 16:45:37   Power up system reset
10/2/97 16:45:37   Bridge enable port 0:1 VC 0
10/2/97 16:45:37   IP port on 0 to 0.0.0.0 available
10/2/97 16:45:37   SRAM erased!! Cnfg. JUMPER pulled off or Cold boot!!
10/2/97 16:46:11   Bridge disable port 0:1 VC 0
10/2/97 16:46:11   IP port 0 unavailable
10/2/97 16:46:16   IP port on 0 to 0.0.0.0 available
10/2/97 17:05:16   IP port 3 unavailable



Enter Y<RET> or <RET> to clear the system error log, otherwise N<RET> :
```

Figure 20-35 System Error Log

The log is displayed one page at a time; pressing **<return>** displays the next page. When you reach the end of the log, you must press either **Y** or **N** followed by **<return>** to exit. Entering **Y** will clear the log. Entering **N** will keep the log as it is. Please note that if the log fills up, new error messages will be discarded.

Some of the messages you might see in the System Error Log are explained below:

Port n is down (ddd).

The port numbered *n* has gone to a down status. The reason is given by a diagnostic code. Diagnostic codes are provided in Table 20-24.

Dial port n is not responding to configure.

The dial modem is not returning a result to the Configure command.

Error configuring modem on port n.

The dial modem returned an error result in response to the Configure command.

Unrecognized modem result m on port n.

The modem has signaled an unrecognized result code for an incoming call.

File server is not available.

Ethernet broadcast frames have not been received from the file server for 5 minutes.

The System Error Log retains the most recent 32 KB of error messages and discards the oldest messages when the log fills.

NOTE: So that you do not lose any error log messages, it is a good idea to clear the error log at regular intervals.

Table 20-24 lists the diagnostic codes that can be received on a port down message.

Table 20-24 “Port Down” Diagnostic Codes

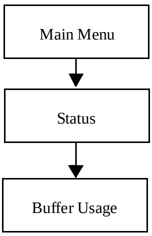
Port Types/Code	Meaning
All ports	
160	Disabled by administrator
Async-in	
192	Data set signals dropped
193	Maximum retransmissions received
194	ID string not received
Async-out	
196	Client workstation cleared connection
PAD, console & async-out over X.25	
128	Data set signals dropped
129	Connection timeout expired

Table 20-24 “Port Down” Diagnostic Codes (cont.)

Port Types/Code	**Meaning**
130	User disconnected call (using X.28 Clear command)
131	User reset call (using X.28 Reset command)
132	Distant device sent X.29 Invitation to Clear message
133	Distant device sent X.29 Reselect message
134	Reset sent on break (X.3 Parameter 7)
135	Timeout on data inactivity
PPP & X.25 & frame relay	
144	Data set signals dropped
PPP & X.25	
145	Received Disconnect command
146	Received Disconnect mode response
148	Timeout on configuring modem
X.25	
147	N2 retransmissions
152	Link congested
PPP	
154	No echo received
Frame relay	
154	No LMI received
Ethernet	
195	Ethernet broadcast not received

■ BUFFER USAGE

The Buffer Usage screen provides information on the number of available buffers and the number of free buffers. This information can be used by your *DYNASTAR* technical support representative for troubleshooting. The Buffer Usage screen is shown in Figure 20-36.




```
                         *** Buffer Usage ***

   Number of Buffers in Use =                3
   Number of FREE Buffers in pool =       8199
   Number of Free Buffers in ISR =          64
   Number of Buffers in Total =           8267
   System idle count =                   10655

   Daughterboard 1: Idle = 41932 Number of buffers = 2528 (2528 in pool)
   Daughterboard 2: Idle = 41932 Number of buffers = 100 (100 in pool)
   Daughterboard 3: Idle = 41932 Number of buffers = 100 (100 in pool)
   Daughterboard 4: Idle = 41932 Number of buffers = 100 (100 in pool)

   DIMM installed:  16 Mbyte
   Chassis internal temperature:  45.0 C = 113.0 F



_______[DynaStar_399c]_______
Press ESC to return to previous menu.             Press <RET> for update.
```

Figure 20-36 Buffer Usage Screen

TROUBLESHOOTING

21

This chapter provides instructions on how to troubleshoot the *DYNASTAR* from the Supervisor Console. Information reported to the Supervisor Console is used to determine the cause of a system failure or degraded performance condition.

■ TROUBLESHOOTING OVERVIEW

DYNASTAR errors fall into the following general categories:

- Incorrect version of support software or incorrect ROM on baseboard
- Remote workstation/async device-to-*DYNASTAR* connection problems
- Remote workstation-to-file server connection problems
- Supervisor Console-to-*DYNASTAR* connection problems
- *DYNASTAR*-to-*DYNASTAR* direct synchronous connection problems
- X.25 network-to-*DYNASTAR* connection problems
- Frame relay network-to-*DYNASTAR* connection problems

INCORRECT SUPPORT SOFTWARE OR ROM VERSIONS

Application software for the *DYNASTAR* is distributed on a PC disk and is downloaded to the on-board flash, which is controlled by an on-board ROM. As new application software versions are released, changes may also be made in the ROM.

If you are experiencing difficulties with the *DYNASTAR*, check the Login screen to determine what version of software is loaded and use the Applications menu (Main/System Functions/Applications) to verify that the correct ROM is installed. If the **ROM Installed** field shows an older version than the version specified in the **ROM Required** field, contact your service representative.

REMOTE IPX WORKSTATION-TO-ACCESS SERVER CONNECTION

When the remote workstation is unable to make a successful connection to the access server, the following NetWare IPX message is displayed on the remote workstation's console:

Invalid ID String: Network access denied.

To isolate the problem for a direct or leased line connection, perform the following steps:

Check cable	Check that the cable is connected to the correct port on the access server. For a direct connection, you can also check that the cable is connected to the correct PC COM port on the remote workstation.
Check RS-232 adapter	For a leased line connection, check that the correct RS-232 adapter configuration (DTE) is used at the asynchronous modem. For a direct connection, check that the correct RS-232 adapter configuration (DCE) is used at the remote PC COM port at the remote workstation.
Check port configuration	Use the Status/Board menu to check that the port is configured and enabled. Use the Configure/Port menu to check the value of individual configuration parameters.
Check data set signals	Use the Status/Statistics menu to check that there is at least one incoming data set signal. If there is no data set signal, either the cable is not plugged into the correct port or the cable/RS-232 adapter is bad.

Check for characters being received	Use the Status/Statistics menu to check that characters are being received. If not, either the cable is not plugged into the correct port, or the cable/RS-232 adapter is bad.
Check for character errors	Use the Status/Statistics menu to check that characters are being received with no breaks or framing errors. Breaks and framing errors indicate a speed mismatch.
Check ID string	Use the Status/Log menu to identify an ID string mismatch. Use the Access Server menu to obtain a list of valid ID strings for the access server.

To isolate the problem for a dial connection, perform the following steps:

Check cable	Check that the cable is connected to the modem and to the correct port on the access server.
Check RS-232 adapter	Check that the correct RS-232 adapter configuration (DTE) is used at the asynchronous modem.
Check port configuration	Use the Status/Board menu to check that the port is configured and enabled. Use the Configure/Port menu to check the value of individual configuration parameters.
Check modem configuration	Use the Status/Log menu to identify any modem configuration. Use the Configure/Port menu to check the value of modem configuration parameters.
Check that the modem answers	Check that the modem answers the incoming call. If the call is not answered, the modem has not been configured correctly. See the user guide that came with your modem.
Check for immediate disconnect	Use the Status/Log menu to check for a port down diagnostic code 192. If present, it indicates that the access server does not detect the Carrier Detect (CD) data set signal and has disconnected the call. If CD cannot be detected, either the cable/RS-232 adapter is bad, or the modem is configured incorrectly.

Check for characters being received	Use the Status/Statistics menu to check that characters are being received. If not, the cable is not plugged into the correct port, or the cable/RS-232 adapter is bad.
Check for character errors	Use the Status/Statistics menu to check that characters are being received with no breaks, framing, or parity errors. Breaks and framing errors indicate a speed mismatch. Parity errors indicate that the modem did not signal (via a result code) that the call was successfully connected. Use the Status/Log menu to identify modem result code errors. For proper modem configuration, see the user guide that came with your modem.
Check ID string	Use the Status/Log menu to identify an ID string mismatch. Use the Configure/Access Server menu to get a list of valid ID strings for the access server.

Remote Workstation-to-File Server Connection

After the remote workstation makes a connection to the access server, it automatically attempts to attach to the nearest file server. If a file server is not available, the following NetWare IPX message is displayed on the remote workstation's console:

A File Server could not be found.

To isolate the problem, perform the following steps:

Check the Ethernet port status	Use the Status/Board menu to check that the LAN port is enabled and operational (up).
Check file server availability	Use the Status/Statistics menu to check that the file server is available on the LAN by monitoring the counts of broadcast frames. If there is no file server traffic, make sure that the file server is operational. If the file server is operational, use the Track command on the file server's console to verify communication between the access server and file server.

Whenever a line error occurs on the async line, either the access server or the remote workstation retransmits the missing IPX frame. After multiple retransmissions, the connection is declared down. Use the Status/Log menu to check the reason that the port went down.

The IPX frame can be successfully transmitted over the async line and then lost on the LAN. In this case, either the file server or the remote workstation retransmits the IPX frame. After one retransmission, the remote workstation declares a network error, and the following NetWare IPX message is displayed on the remote workstation's console:

Network Error on Server sss: Error receiving from network. Abort, Retry?

If the error is only a momentary transmission error, the connection continues when the user enters **r** for retry. If the error is a result of the communication path to the access server's being disconnected, the network error message is displayed again with this description:

Error locating router.

In this case, you must enter **a** for abort and then reboot the remote workstation to make another connection to the access server.

ACCESS SERVER-TO-REMOTE DEVICE CONNECTION

When a workstation is unable to make a successful connection to a remote device, the application displays an appropriate error message on the workstation's console.

To isolate the problem for a direct or leased line connection, perform the following steps:

Check cable	Check that the cable is connected to the correct port on the access server. For a direct connection, also check the cable connection at the asynchronous device.
Check RS-232 adapter	For a leased line connection, check that the correct RS-232 adapter configuration (DTE) is used at the asynchronous modem. For a direct connection, check that the correct RS-232 adapter configuration (DCE) is used at the asynchronous device.
Check port configuration	Use the Status/Board menu to check that the port is configured and enabled. Use the Configure/Port menu to check the value of individual configuration parameters.
Check data set signals	Use the Status/Statistics menu to check that there is at least one incoming data set signal. If there is no data set signal, either the cable is not plugged into the correct port, or the cable/RS-232 adapter is bad.
Check for characters being received	Use the Status/Statistics menu to check that characters are being received. If not, either the cable is not plugged into the correct port, or the cable/RS-232 adapter is bad.
Check for character errors	Use the Status/Statistics menu to check that characters are being received with no breaks or framing errors. Breaks and framing errors indicate a speed mismatch.
Check passwords	Use the Configure/Access Server menu to get a list of services that require a password.

To isolate the problem for a dial connection, perform the following steps:

Check cable	Check that the cable is connected to the modem and to the correct port on the access server.
Check RS-232 adapter	Check that the correct RS-232 adapter configuration (DTE) is used at the asynchronous modem.
Check port configuration	Use the Status/Board menu to check that the port is configured and enabled. Use the Configure/Port menu to check the value of individual configuration parameters.
Check modem configuration	Use the Configure/Port menu to check the value of modem configuration parameters.
Check for immediate disconnect	Use the Status/Log menu to check for a port down diagnostic of 192. If present, it indicates that the access server does not detect the Carrier Detect (CD) data set signal and has disconnected the call. If CD cannot be detected, either the cable/RS-232 adapter is bad, or the modem is configured incorrectly.
Check for characters being received	Use the Status/Statistics menu to check that characters are being received. If no characters are being received, either the cable is not plugged into the correct port, or the cable/RS-232 adapter is bad.
Check for character errors	Use the Monitor command to check that characters are being received with no breaks, framing, or parity errors. Breaks and framing errors indicate a speed mismatch.
Check passwords	Use the Configure/Access Server menu to obtain a list of services that require a password.

Supervisor Console-to-*DynaStar* Connection

If there is no output to the console, perform the following steps to isolate the problem:

Check cable	Check that the cable is connected to the terminal and to the correct port on the *DynaStar*.
Check RS-232 adapter	Check that the correct RS-232 adapter configuration (DCE) is used at the terminal.
Check port configuration	Check that the port is configured and enabled. The internal communications module may have a hardware error.
Check data set signals	Use an RS-232 breakout box to check that there is at least one incoming data set signal. No data set signals indicates that the cable/RS-232 adapter is bad.
Check character transmission	Use an RS-232 line monitor to check that characters are being sent and received.

If the above steps do not isolate the problem, the console port may be configured incorrectly in software tables. Call your service representative for assistance.

Synchronous Connection

If the connection between a pair of *DynaStars* fails, perform the following steps to isolate the problem:

Check cable	Check that the cable is connected to the synchronous modem and to the correct port on the *DynaStar*.
Check adapter	Check that the correct cable configuration (DTE) is used at the modem.
Check port configuration	Use the Status/Board menu to check that the port is configured and enabled. Use the Configure/Port menu to check the value of individual configuration parameters.

Check data set signals	Use the Status/Statistics menu to check that there is at least one incoming data set signal. If there is no data set signal, either the cable is not plugged into the correct port, or the cable/adapter is bad.
Check frame transmission	Use the Status/Statistics menu to check that frames are being transmitted. If there are both T1 timeouts and transmit failures, there is no clock from the modem. This indicates that either the cable/adapter is bad or that there is no clock source.
Check frame reception	Use the Status/Statistics menu to check that frames are being received. If not, either the cable or adapter is bad.

X.25 Network-to-*DynaStar* Connection

When an X.25 PDN is connected to an X.25 line port, the X.25 software of the *DynaStar* automatically initiates a connection to the PDN for any bridge or router calls that are properly configured.

If the connection attempt is not successful, perform the following steps to isolate the problem:

Check cable	Check that the cable is connected to the synchronous modem and to the correct port on the *DynaStar*.
Check adapter	Check that the correct adapter configuration (DTE) is used at the modem.
Check port configuration	Use the Status/Board menu to check that the port is configured and enabled. Use the Configure/Port menu to check the value of individual configuration parameters. In particular, make sure that the X.25 mode DCE/DTE setting is correct.

Check data set signals	Use the Monitor command to check that there is at least one incoming data set signal. If there is no data set signal, the cable is not plugged into the correct port, or the cable/adapter is bad.
Check frame transmission	Use the Status/Statistics menu to check that frames are being transmitted. If there are both T1 timeouts and transmit failures, there is no clock from the modem. This indicates that either the cable/adapter is bad or the modem is not providing clock.
Check frame reception	Use the Status/Statistics menu to check that frames are being received. If not, either the cable or adapter is bad.

If the X.25 link is up, but traffic is slow, check the following:

Check the DTE/DCE configuration.	The DTE/DCE clocking could be misconfigured. Be sure that one end of the link is configured as a physical DTE and that the other end is configured as a physical DCE.

If the X.25 link is up but X.25 virtual calls to the *DYNASTAR* are not successfully completed, perform the following steps:

Check port configuration	Use the Status/Statistics menu to monitor call attempts. Use the Configure/Port menu to check that the X.25 line port configuration parameters (number of VCs and VC base) match the PDN's configuration parameters. For assistance, call your PDN's service representative.
Check X.25 call statistics	Use the Status/Statistics menu to monitor outbound call attempts; look for character count on inbound calls.
Check X.121 address	Use the Status/Names & Addresses menu to verify the destination's X.121 address. Make sure that the X.121 address is correct and configured properly at the remote end of the X.25 virtual call.

DynaStar Approvals

- UL (both US and Canadian [C-UL])
- FCC Part 15, Subpart J
- FCC Part 68
- BABT (Telco for synchronous ports)
- Net1 (X.21)
- Net2 (X.25 Levels 2 and 3, V.35, and V.24)
- EN 41003 and EN 60950 (safety and protection)
- EN 55022, IEC 801 Parts 2, 3, and 4 (EMC)
- IEC 61000-4-4 and IEC 6100-4-5 Damped Oscillation Waveform Test
- IEEE C 37.90.1 Standard Surge Withstand Capability (SWC) Tests for Protective Relays
- IEEE C 37.90.2 Withstand Radiated Electromagnetic Interference from Transceivers
- IEEE C 37.90.3 Standard Electrostatic Discharge for Protective Relays
- NEBS, Parts of GR-1089-CORE, including ESD, EMI emissions, EMI immunity, lightning and AC power fault on Telco and power lines, electrical safety, and power and grounding
- NEBS, Parts of GR-63-CORE, including temperature, humidity, altitude, fire resistance, handling, transportation, and vibration
- RFC 1717 PPP Multilink Protocol
- RFC 1662 PPP in HDLC-like Framing
- RFC 1661 The Point-to-Point Protocol
- RFC 1634 Novell IPX over Various WAN Media

- RFC 1613 Cisco Systems X.25 over TCP (XOT)
- RFC 1552 The PPP Internetwork Packet Exchange Control Protocol (IPXCP)
- RFC 1505 Encoding Header Field for Internet Messages
- RFC 1493 Definition of Managed Objects for Bridges
- RFC 1490 Multiprotocol Interconnect over Frame Relay
- RFC 1483 Multiprotocol Encapsulation over ATM Adaptation Layer 5
- RFC 1356 Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode
- RFC 1350 The TFTP Protocol (Revision 2)
- RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
- RFC 1213 Management of Information Basic for Network Management of TCP/IP-based Internets: MIB-II
- RFC 1157 A Simple Network Management Protocol (SNMP)
- RFC 1155 Structure and Identification of Management Information for TCP/IP-based Internets
- RFC 1091 Telnet Terminal-type Option
- RFC 1055 Nonstandard for Transmission of IP Datagrams over Serial Lines-SLIP
- RFC 1042 Standard for the Transmission of IP Datagrams over IEEE 802 Networks
- RFC 857 Telnet Echo Option
- RFC 856 Telnet Binary Transmission
- RFC 855 Telnet Option Specifications
- RFC 854 Telnet Protocol Specification
- RFC 826 Ethernet Address Resolution Protocol
- RFC 792 Internet Control Message Protocol

- RFC 791 Internet Protocol
- RFC 768 User Datagram Protocol

CABLES AND CONNECTORS

Table B-1
Maximum DTE Cable Lengths

DTE Data Rate	Maximum Cable Length, Feet			
(kbps)	**RS232C**	**V.35**	**RS449/422**	**RS530/422**
56 or 64	10	4000	4000	4000
112 or 128	N/A	4000	3800	3800
224 or 256	N/A	3500	1700	1700
448 or 512	N/A	2500	700	700
896 or 1024	N/A	1700	350	350
1344 or 1536	N/A	600	200	200

N/A: Not applicable. These rates cannot be used for RS232C interfaces.

Table B-2
Pin/Signal Assignments on the DB-15 Connector for V.35 Operation

DB-15 Pin	Signal Descriptions	V.35 Pin
2	Transmit Data (A)	P
9	Transmit Data (B)	S
4	Receive Data (A)	R
11	Receive Data (B)	T
5	Transmit Clock (A)	Y
12	Transmit Clock (B)	AA
6	Receive Clock (A)	V
13	Receive Clock (B)	X
14	Data Terminal Ready	H
3	Request to Send	C
10	Data Carrier Detect	F
15	Clear to Send	D
7	Data Set Ready	E
8	Signal Ground	B
1	Chassis Ground	A

Table B-3
Pin/Signal Assignments on the
DB-15 Connector for X.21 Operation

DB-15 Pin	Signal Description	X.21 Pin
2	Transmit Data (A)	TA
9	Transmit Data (B)	TB
4	Receive Data (A)	RA
11	Receive Data (B)	RB
6	Clock (A)	SA
13	Clock (B)	SB
3	Control (A)	CA
10	Control (B)	CB
5	Indication (A)	IA
12	Indication (B)	IB
8	Signal Ground	G
1	Chassis Ground	CG
7	Not used	
14	Not used	
15	Not used	

Table B-4
Pin/Signal Assignments on the DB-15 Connector for RS-232/V.24 Operation

DB-15 Pin	Signal Description
1	Chassis Ground
2	TxD
3 *	RTS
4	RxD
5 *	TxCLKA
6 *	RxCLKA
7	DSR
8	Signal Ground
9	Not used
10 *	DCD
11	Not used
12	Not used
13	Not used
14	DTR
15 *	CTS

* Not used by the *DYNASTAR 100e* or *DYNASTAR 2000* Alarm port or the *DYNASTAR 5000* Debug port.

Table B-5
Pin/Signal Assignments on
RJ-45 and RJ-69 Connectors for Synchronous and Asynchronous Operation

RJ-45 Pin	RJ-69 Pin	SYNC/ ASYNC and 16-Port Board	Console
X	1	Tx Clock	Not Used
1	2	RTS	RTS
2	3	DSR*	DSR*
3	4	TxD	TxD
4	5	RxD	RxD
5	6	GND	GND
6	7	DTR	DTR
7	8	DCD	DCD
8	9	CTS	CTS
X	10	Rx Clock	Not Used

* When port configured as DTE: DSR input not used.
When port configured as DCE: DSR is an output.

NOTE: RJ-69 connectors are also known as 10-pin RJ-45.

Table B-6
Pin/Signal Asignments
on the RJ-45 for Dual BRI

RJ-45 Pin	S-Interface Signal	U-Interface Signal
1	Not Used	Not Used
2	Not Used	Not Used
3	Tx Tip	Not Used
4	Rx Tip	Tip
5	Rx Ring	Ring
6	Tx Ring	Not Used
7	Not Used	Not Used
8	Not Used	Not Used

Table B-7
Pin/Signal Assignments on the
RJ-48 Connector for T1 and E1 Interfaces

RJ-48 Pin	Signal Description
1	T1 Receive +
2	R1 Receive -
3	Shield
4	T Transmit +
5	R Transmit -
6	Shield
7	not used
8	not used

Table B-8
Pin/Signal Assignments on the RJ-48 Connector for DDS

RJ-48 Pin	Signal Description
1	Tx Data (Ring)
2	Tx Data (Tip)
3	N/C
4	N/C
5	N/C
6	N/C
7	Rx Data (Tip)
8	Rx Data (Ring)

Table B-9
Pin/Signal Assignments on the
DB-15 Connector for T1 and E1 Interfaces

DB-15 Pin Female DCE	DB-15 Pin Male DTE	Signal Description *
3	1	Transmit T
11	9	Transmit R
1	3	Receive T1
9	11	Receive R1

* All other pins unused.

Table B-10
Pin/Signal Assignments on the
RJ-45 Connector for Ethernet Interfaces

RJ-45 Pin	Signal Description
1	Transmit +
2	Transmit -
3	Receive +
4	Not Used
5	Not Used
6	Receive -
7	Not Used
8	Not Used

Table B-11
PinAssignments on the RS-485 Interface

RS-485 Pin	Circuit Definition
1, 16, 17	Chassis Ground
8	Signal Ground
2 (B), 9 (A)	4-wire Rx or 2-wire Tx/Rx
4 (B), 11 (A)	4-wire Tx

Table B-12
Pin/Signal Assignments on the DB-15 Connector for the *DYNASTAR 100e* and *DYNASTAR* 2000 Alarm Ports

DB-15 Pin Female DCE	Signal Description *
1	Chassis Ground
2	TxD
3	RTS
4	RxD
5	Normally Open Alarm Relay
6	Normally Closed Alarm Relay
7	DSR
8	Signal Ground
9	Not Used
10	DCD
11	Not Used
12	Not Used
13	Common Alarm Relay
14	DTR
15	CTS

* Includes the debug test port signals.

Table B-13
Pin/Signal Assignments on the External Alarm Port on the *DynaStar 500* and the *DynaStar 5000*

Mini DIN Pin	Pin Number on Relay One	Pin Number on Relay Two
1	4 (NO)	N/A
2	3 (COM)	N/A
3	2 (NC)	N/A
4	N/A	2 (NC)
5	N/A	3 (COM)
6	N/A	4 (NO)

The pinout on this connector is non-standard. Please refer to the diagram in Figure B-6.

.

Table B-14
V.24 DB-15 Conversion to RS-232/V.24 DB-25
Part No. 160-0542-001 (Male)
Part No. 160-0543-001 (Female)

DB-15 Connector	DB-25 Connector	Signal
1	1	Frame Ground
2	2	TxD
3	4	RTS
4	3	RxD
5	15	TxC
6	17	RxC
7	6	DSR
8	7	Signal Ground
9	n/c	unused
10	8	unused
11	n/c	unused
12	n/c	unused
13	n/c	unused
14	20	DTR
15	5	CTS

Table B-15
DB-15 to DB-25 Pin Correlation
Part No. 160-0545-001

DB-15 Connector	DB-25 Connector
1	1
2	12
3	4
4	13
5	16
6	18
7	6
8	7
9	2
10	8
11	3
12	15
13	17
14	20
15	5

Table B-16
RJ69-to-DB25 Pin Correlation
Part Number 160-0536-001 (Male Adaptor)
Part Number 160-0537-001 (Female Adaptor)

RJ69	DB25	Signal
1	15	Tx Clock
2	4	RTS
3	6	DSR
4	2	TxD
5	3	RxD
6	7	Signal Ground
7	20	DTR
8	8	DCD
9	5	CTS
10	17	Rx Clock

■ CONNECTOR PIN LOCATIONS

The following figures are provided to help you identify pin locations on *DYNASTAR* connectors. All numbering is shown looking into the connector from the rear of the *DYNASTAR*.

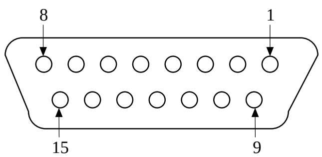


Figure B-1 **DB-15 Connector (Female)**

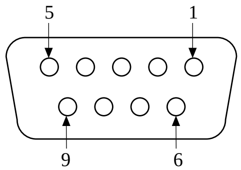


Figure B-2 **DB-9 Connector (Female)**

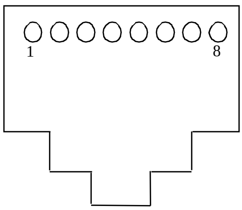


Figure B-3 **RJ-45 Connector and RJ-48 Connector**

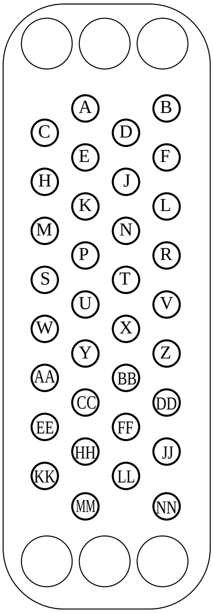


Figure B-4 V.35 Connector

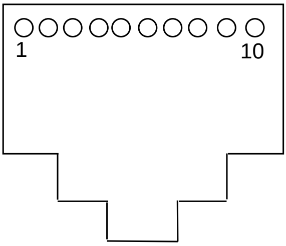


Figure B-5 RJ-69 Connector (Sometimes Called 10-Pin RJ-45)

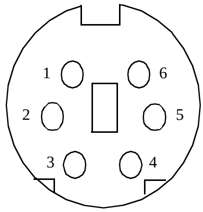


Figure B-6 ***DynaStar 500*** **External Alarm Connector (note non-standard numbering)**

SNMP

■ Setting SNMP Parameters

A system administrator can use a standard SNMP manager to access the *DynaStar* SNMP agent to:

- Monitor the status of the *DynaStar*
- Monitor the status of individual ports and calls
- Read configuration parameters defined by standard MIBs
- Read and set configuration parameters defined by the enterprise MIB
- Enable and disable ports
- Warm or cold start the *DynaStar*

The enterprise MIB contains the configuration variables that can be read and set and the status variables that can be read using the Supervisor, with the following exceptions:

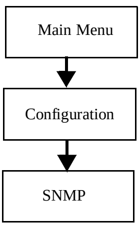
- The Supervisor's password cannot be set.
- SNMP community string passwords and authentication cannot be read or set.
- Optional applications cannot be activated or deactivated.
- Software downloads/uploads cannot be initiated.

Before an SNMP manager can be connected to the SNMP agent, you must make certain that you have enabled IP capabilities in the network. This means that the proper IP addressing has been assigned to any *DynaStars* that are to be managed through an SNMP manager. In addition, unless an alternate path is provided, IP routing must be enabled on the Ethernet Port Configuration menu (from the Main menu, select **Configuration**, then **Port**, then **Port 0**).

SNMP Variable Descriptions

To view or change SNMP parameters, access the SNMP Parameters screen, shown in Figure C-1. The SNMP parameters and values are defined in Table C-1.

NOTE: If you do not set any SNMP parameters, all MIBs are read-only, and no traps are enabled.




```
                              ***SNMP Parameters***
                                                  Last changed:  4-23-02  11:26:45

 ------------------------------Enter a maximum of 48 characters--------------------------------------
System description:    DynaStar 500
System contact:
System name:
System location:
Read-Only Community name:
Read-Write Community name:
Private Community name:

--------------------------Enter 4 integers, 0-255, separated by a period----------------------------
Trap IP Address:      0.0.0.0                    Trap IP Address:      0.0.0.0
Trap IP Address:      0.0.0.0                    Trap IP Address:      0.0.0.0

--------------------------------------Use RET to toggle value---------------------------------------------
Enable authentication:     N
Enable traps:              N
GUI Display Type (for DynaStar 100/100i): not applicable

 ________[DynaStar_3614]_________                  Process selections (Y/N): Y
 To change or add entry, enter new value.          Use <CTRL-D> to delete entry.
Use TAB & CURSOR keys to move among fields.        Press ESC to abort command & exit.
```

Figure C-1 SNMP Parameters Screen

Table C-1 SNMP Parameters

Parameter	Description	Values
System Description	A textual description of the *DYNASTAR* that the Supervisor uses to set the MIB-II sysDescr variable. It should include the full name of the system's hardware type.	*DYNASTAR 500* *DYNASTAR 100* *DYNASTAR 100i* *DYNASTAR 100e* *DYNASTAR 2000* *DYNASTAR 5000*
System Contact	The name of a contact person for the *DYNASTAR* together with information on how to contact this person. It is used by the Supervisor to set the MIB-II sysContact variable.	48 characters Default=null
System Name	The identifier for the *DYNASTAR* that the Supervisor has used to set the MIB-II sysName variable.	48 characters Default=null
System Location	The physical location of the *DYNASTAR* (e.g., "telephone closet, 3rd floor"). It is used by the Supervisor to set the MIB-II sysLocation variable.	48 characters Default=null
Read-Only Community Name	Used by the SNMP agent as a simple authentication mechanism for read-only access to all MIBs. If no string is defined, all standard and private MIB information is read-only, and no authentication failure trap is issued.	48 characters Default=null
Read-Write Community Name	Used by the SNMP agent as a simple authentication mechanism for read access to all MIBs and write access to standard MIBs. If no string is defined, all MIB information is read-only, and no authentication failure trap is issued.	48 characters Default=null

Table C-1 SNMP Parameters (cont.)

Parameter	Description	Values
Private Community Name	Used by the SNMP agent as a simple authentication mechanism for read and write access to all MIBs. If no string is defined, all MIB information is read-only, and no authentication failure trap is issued.	48 characters Default=null
Trap IP Address	When a trap condition occurs, the SNMP agent sends an SNMP trap PDU to this address's management station. Addresses can be entered for up to four SNMP managers.	Valid IP address Default=0.0.0.0
Enable Authentication	When set to Y(es), the agent matches the community string on an incoming PDU with community names. If there is no match, no access is allowed. If Enable Traps is also set to Y(es), the agent issues an authentication failure trap. If there is a match, read only or read/write access is allowed, depending on the name matched. When Enable Authentication is set to N(o), no check is made, and read only access to all MIBs is allowed.	Y N=default
Enable Traps	When set to Y(es) and an error condition occurs, the agent sends an SNMP trap PDU to the IP addresses specified as Trap IP addresses. When Enable Traps is set to N(o), no traps are sent.	Y N=default

Table C-1 SNMP Parameters (cont.)

Parameter	Description	Values
GUI Display Type	Used to configure the type of *DYNASTAR 100/100i* that is displayed in the Graphic User Interface.	not applicable (fixed for *DYNASTAR 100e/ 2000/500/5000*) desktop rackmount (default for *DYNASTAR 100*, *DYNASTAR 100i*)

SNMP MANAGER LOCK-OUT

The *DYNASTAR* Private Enterprise MIB's multi-manager lock-out mechanism lets an SNMP manager prevent other managers and the Supervisor from making changes to configuration parameters. When applied, the warning message

*** An SNMP Manager is making configuration changes ***

appears on the top line of the current Supervisor Console screen. If this appears, immediately exit any configuration screen and return to the Main menu.

If you attempt to access the Configuration menu when the lock is set, the message

ACCESS DENIED:
An SNMP Manager is making configuration changes

appears on your screen. While the lock is set, you can use the Status, Applications, and System Reload menus.

The Supervisor cannot inform you when the lock-out mechanism has been reset. If you need to make configuration changes, periodically try to access the Configuration menu until you are given entry.

X.3 PROFILES AND PARAMETERS

■ X.3 PARAMETERS

There are 22 X.3 parameters that define the way the asynchronous ports operate. The X.3 parameters and their possible values are explained in Table D-1.

Table D-1
X.3 Parameters

Parameter Number and Name	Description	Possible Values
1 PAD Recall Char	Indicates whether the terminal can communicate directly with the PAD.	0 - Not possible 1 - Possible using DLE (Ctrl-P) char. 2-127 - Possible using selected character
2 Echo	Indicates whether there is a local echo.	0 - No echo 1 - Echo
3 Data Forwarding Characters	Indicates what characters will signal that data should be forwarded.	0 - No data forwarding chars. 2 - CR 16 - EXT, EOT 18 - EXT, EOT, CR 126 - All chars + DEL 127 - Forward on every character 128+n -Forward after n characters

Table D-1
X.3 Parameters (cont.)

Parameter Number and Name	Description	Possible Values
4 Idle Timer	Indicates that a partially filled packet will be forwarded if nothing is received from the terminal for this amount of time.	0-250, the specified number is in one-twentieths of a second Also, special values: 251 - 3-10 ms 252 - 20 ms 253 - 30 ms 254 - 40 ms 255 - 50 ms
5 PAD to Terminal Flow Control	Indicates if the PAD can send flow control signals to the terminal.	0 - No XON, XOFF 1 - XON, XOFF in data transfer mode 2 - XON, XOFF in data transfer and command modes
6 Control of PAD Service Signals	Indicates whether PAD service signals (messages) are sent from the PAD to the terminal.	0 - Signals not sent 1 - Standard signals sent 5 - Signals + prompt sent
7 PAD Action on Receipt of Break	Indicates how the PAD reacts when it receives a Break signal.	0 - Do nothing 1 - Send Interrupt packet 2 - Reset 8 - Escape from data transfer mode 21 - Discard output and send Interrupt packet and Break
8 Disregard output	Works in conjunction with parameter 7 to indicate what to do with any output.	0 - Normal data delivery 1 - Discard output
9 Padding after CR	Indicates what padding, if any, is used after a carriage return.	0 - No padding 1-7 One to seven NULLs, as indicated

Table D-1
X.3 Parameters (cont.)

Parameter Number and Name	**Description**	**Possible Values**
10 Line Folding	Indicates the number of characters to have per line.	0 - No line folding 1-255 The number of characters per line
11 Baud Rate	The terminal speed. This is a read-only parameter.	0 - 110 bps 2 - 300 bps 3 - 1200 bps 4 - 600 bps 5 - 75 bps 13 - 4800 bps 14 - 9600 bps 15 - 19200 bps
12 Terminal to PAD Flow Control	Indicates if the terminal can send flow control signals to the PAD.	0 - No XON, XOFF 1 - XON, XOFF
13 Linefeed Insertion	Indicates whether a linefeed is inserted after a CR.	0 - No LF 1 - LF inserted after CR transmitted to DTE 2 - LF inserted after CR from the DTE 4 - LF inserted after CR echo 5 - 1+4 6 - 2+4 7 - 1+2+4
14 Padding after Linefeed	Indicates whether any padding is inserted after an LF.	0 - No padding 1-7 Send the specified number of Null characters (Data transfer mode only)
15 Editing	Indicates whether or not editing is allowed at the terminal.	0 - No editing 1 - Editing in data transfer mode
16 Character delete	Indicates which character is used as the character delete function.	0-126 Specified character from IA5 127 - DEL

Table D-1
X.3 Parameters (cont.)

Parameter Number and Name	Description	Possible Values
17 Line Delete	Indicates which character is used as the line delete function.	0-23 Specified character from IA5 24 - CAN 25-127 Specified character from IA5
18 Line Display	Indicates which character is used for the line display function.	0-17 Specified character from IA5 18 - DC2 19-127 Specified character from IA5
19 Editing PAD Service Signals	Indicates whether the service signals can be edited.	0 - No editing 1 - Editing for printing terminals 2 - Editing for display terminals
20 Echo Mask	Indicates which characters are not echoed.	0 - No mask 1 - CR 2 - LF 4 - VT, HT, FF 8 - BEL, BS 16 - ESC, ENQ 32 - ACK, NAK, STX, SOH, EOT, ETB, ETX 64 - No echo of chars defined by parameters 16, 17, 18 128 - No echo of characters not listed above + DEL
21 Parity Treatment	Indicates whether parity is checked or generated.	0 - Neither 1 - Checking 2 - Generation
22 Page Wait	Indicates the number of LFs that constitute a page.	0 - No page wait 1-255 LFs used by the PAD for the page wait function

Table D-2
Parameter Settings for
Standard ITU-T (CCITT) Profiles

Parameter	Parameter Name	ITU-T Simple (Profile 90)	ITU-T Transparent (Profile 91)
1	PAD recall	1	0
2	PAD echo	1	0
3	Data forwarding rate	126	0
4	Idle timer	0	20
5	Flow control by PAD	1	0
6	PAD service signals	1	0
7	Break handling	2	2
8	Discard output	0	0
9	Padding after CR	0	0
10	Line folding	0	0
12	Flow control of PAD	1	0
13	LF after CR	0	0
14	Padding after LF	0	0
15	Editing	0	0
16	Character delete	127	127
17	Line delete	24	24
18	Line display	18	18
19	Editing signals	1	1
20	Echo mask	0	0
21	Parity treatment	0	0
22	Page wait	0	0

Table D-3 Parameter Settings for Standard ACT Networks Profiles

Parameter	Parameter Name	LAN (Profile 86)	Telnet (Profile 87)	TTY (Profile 88)	CRT (Profile 89)
1	PAD recall	0	0	1	1
2	PAD echo	0	0	1	1
3	Data forward-ing rate	0	0	2	2
4	Idle timer	1	1	0	0
5	Flow control by PAD	0	1	1	1
6	PAD service signals	0	0	5	5
7	Break handling	0	0	0	0
8	Discard output	0	0	0	0
9	Padding after CR	0	0	0	0
10	Line folding	0	0	0	0
12	Flow control of PAD	0	1	1	1
13	LF after CR	0	0	0	4
14	Padding after LF	0	0	0	0
15	Editing	0	0	1	1
16	Character delete	0	0	127	127
17	Line delete	0	0	24	24
18	Line display	0	0	18	18
19	Editing signals	0	0	1	2
20	Echo mask	0	0	240	240
21	Parity treat-ment	0	3	3	3
22	Page wait	0	0	0	0

CONTACT MODULE

Contact module connections for each slot and for each RJ-45 pair are given in Table E-1. Technical specifications follow.

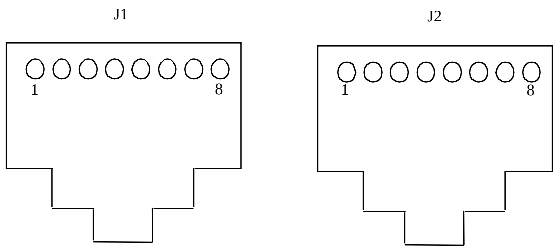


Figure E-1 Contact Module Connectors J1 and J2

Table E-1
Contact Module Connector Pinouts for Each Slot

Pin	SLOT 1	SLOT 2	SLOT 3	SLOT 4	SLOT 5
A-J1					
1	C2_RTN	C50_RTN	C98_RTN	C146_RTN	C194_RTN
2	C2_IN	C50_IN	C98_IN	C146_IN	C194_IN
3	C3_RTN	C51_RTN	C99_RTN	C147_RTN	C195_RTN
4	C1_IN	C49_IN	C97_IN	C145_IN	C193_IN
5	C1_RTN	C49_RTN	C97_RTN	C145_RTN	C193_RTN
6	C3_IN	C51_IN	C99_IN	C147_IN	C195_IN
7	C4_RTN	C52_RTN	C100_RTN	C148_RTN	C196_RTN
8	C4_IN	C52_IN	C100_IN	C148_IN	C196_IN

Table E-1
Contact Module Connector Pinouts for Each Slot (cont.)

A-J2

1	C6_RTN	C54_RTN	C102_RTN	C150_RTN	C198_RTN
2	C6_IN	C54_IN	C102_IN	C150_IN	C198_IN
3	Relay 1 NO	Relay 9 NO	Relay 17 NO	Relay 25 NO	Relay 33 NO
4	C5_RTN	C53_RTN	C101_RTN	C149_RTN	C197_RTN
5	C5_IN	C53_IN	C101_IN	C149_IN	C197_IN
6	Relay 1 NO	Relay 9 NO	Relay 17 NO	Relay 25 NO	Relay 33 NO
7	Relay 1 NC	Relay 9 NC	Relay 17 NC	Relay 25 NC	Relay 33 NC
8	Relay 1 NC	Relay 9 NC	Relay 17 NC	Relay 25 NC	Relay 33 NC

B-J1

1	C8_RTN	C56_RTN	C104_RTN	C152_RTN	C200_RTN
2	C8_IN	C56_IN	C104_IN	C152_IN	C200_IN
3	C9_RTN	C57_RTN	C105_RTN	C153_RTN	C201_RTN
4	C7_IN	C55_IN	C103_IN	C151_IN	C199_IN
5	C7_RTN	C55_RTN	C103_RTN	C151_RTN	C199_RTN
6	C9_IN	C57_IN	C105_IN	C153_IN	C201_IN
7	C10_RTN	C58_RTN	C106_RTN	C154_RTN	C202_RTN
8	C10_IN	C58_IN	C106_IN	C154_IN	C202_IN

B-J2

1	C12_RTN	C60_RTN	C108_RTN	C156_RTN	C204_RTN
2	C12_IN	C60_IN	C108_IN	C156_IN	C204_IN
3	Relay 2 NO	Relay 10 NO	Relay 26 NO	Relay 26 NO	Relay 34 NO
4	C11_RTN	C59_RTN	C107_RTN	C155_RTN	C203_RTN
5	C11_IN	C59_IN	C107_IN	C155_IN	C203_IN
6	Relay 2 NO	Relay 10 NO	Relay 18 NO	Relay 26 NO	Relay 34 NO
7	Relay 2 NC	Relay 10 NC	Relay 18 NC	Relay 26 NC	Relay 34 NC
8	Relay 2 NC	Relay 10 NC	Relay 18 NC	Relay 26 NC	Relay 34 NC

Table E-1
Contact Module Connector Pinouts for Each Slot (cont.)

C-J1					
1	C14_RTN	C62_RTN	C110_RTN	C158_RTN	C206_RTN
2	C14_IN	C62_IN	C110_IN	C158_IN	C206_IN
3	C15_RTN	C63_RTN	C111_RTN	C159_RTN	C207_RTN
4	C13_IN	C61_IN	C109_IN	C157_IN	C205_IN
5	C13_RTN	C61_RTN	C109_RTN	C157_RTN	C205_RTN
6	C15_IN	C63_IN	C111_IN	C159_IN	C207_IN
7	C16_RTN	C64_RTN	C112_RTN	C160_RTN	C208_RTN
8	C16_IN	C64_IN	C112_IN	C160_IN	C208_IN
C-J2					
1	C18_RTN	C66_RTN	C114_RTN	C162_RTN	C210_RTN
2	C18_IN	C66_IN	C114_IN	C162_IN	C210_IN
3	Relay 3 NO	Relay 11 NO	Relay 19 NO	Relay 27 NO	Relay 35 NO
4	C17_RTN	C65_RTN	C113_RTN	C161_RTN	C209_RTN
5	C17_IN	C65_IN	C113_IN	C161_IN	C209_IN
6	Relay 3 NO	Relay 11 NO	Relay 19 NO	Relay 27 NO	Relay 35 NO
7	Relay 3 NC	Relay 11 NC	Relay 19 NC	Relay 27 NC	Relay 35 NC
8	Relay 3 NC	Relay 11 NC	Relay 19 NC	Relay 27 NC	Relay 35 NC
D-J1					
1	C20_RTN	C68_RTN	C116_RTN	C164_RTN	C212_RTN
2	C20_IN	C68_IN	C116_IN	C164_IN	C212_IN
3	C21_RTN	C69_RTN	C117_RTN	C165_RTN	C213_RTN
4	C19_IN	C67_IN	C115_IN	C163_IN	C211_IN
5	C19_RTN	C67_RTN	C115_RTN	C163_RTN	C211_RTN
6	C21_IN	C69_IN	C117_IN	C165_IN	C213_IN
7	C22_RTN	C70_RTN	C118_RTN	C166_RTN	C214_RTN
8	C22_IN	C70_IN	C118_IN	C166_IN	C214_IN

Table E-1
Contact Module Connector Pinouts for Each Slot (cont.)

D-J2					
1	C24_RTN	C62_RTN	C120_RTN	C168_RTN	C216_RTN
2	C24_IN	C62_IN	C120_IN	C168_IN	C216_IN
3	Relay 4 NO	Relay 12 NO	Relay 20 NO	Relay 28 NO	Relay 36 NO
4	C23_RTN	C71_RTN	C119_RTN	C167_RTN	C215_RTN
5	C23_IN	C71_IN	C119_IN	C167_IN	C215_IN
6	Relay 4 NO	Relay 12 NO	Relay 20 NO	Relay 28 NO	Relay 36 NO
7	Relay 4 NC	Relay 12 NC	Relay 20 NC	Relay 28 NC	Relay 36 NC
8	Relay 4 NC	Relay 12 NC	Relay 20 NC	Relay 28 NC	Relay 36 NC
E-J1					
1	C26_RTN	C74_RTN	C122_RTN	C170_RTN	C218_RTN
2	C26_IN	C74_IN	C122_IN	C170_IN	C218_IN
3	C27_RTN	C75_RTN	C123_RTN	C171_RTN	C219_RTN
4	C25_IN	C73_IN	C121_IN	C169_IN	C217_IN
5	C25_RTN	C73_RTN	C121_RTN	C169_RTN	C217_RTN
6	C27_IN	C75_IN	C123_IN	C171_IN	C219_IN
7	C28_RTN	C76_RTN	C124_RTN	C172_RTN	C220_RTN
8	C28_IN	C76_IN	C124_IN	C172_IN	C220_IN
E-J2					
1	C30_RTN	C78_RTN	C126_RTN	C174_RTN	C222_RTN
2	C30_IN	C78_IN	C126_IN	C174_IN	C222_IN
3	Relay 5 NO	Relay 13 NO	Relay 21 NO	Relay 29 NO	Relay 37 NO
4	C29_RTN	C77_RTN	C125_RTN	C173_RTN	C221_RTN
5	C29_IN	C77_IN	C125_IN	C173_IN	C221_IN
6	Relay 5 NO	Relay 13 NO	Relay 21 NO	Relay 29 NO	Relay 37 NO
7	Relay 5 NC	Relay 13 NC	Relay 21 NC	Relay 29 NC	Relay 37 NC
8	Relay 5 NC	Relay 13 NC	Relay 21 NC	Relay 29 NC	Relay 37 NC

Table E-1
Contact Module Connector Pinouts for Each Slot (cont.)

F-J1					
1	C32_RTN	C80_RTN	C128_RTN	C176_RTN	C224_RTN
2	C32_IN	C80_IN	C128_IN	C176_IN	C224_IN
3	C33_RTN	C81_RTN	C129_RTN	C177_RTN	C225_RTN
4	C31_IN	C79_IN	C127_IN	C175_IN	C223_IN
5	C31_RTN	C79_RTN	C127_RTN	C175_RTN	C223_RTN
6	C33_IN	C81_IN	C129_IN	C177_IN	C225_IN
7	C34_RTN	C82_RTN	C130_RTN	C178_RTN	C226_RTN
8	C34_IN	C82_IN	C130_IN	C178_IN	C226_IN
F-J2					
1	C36_RTN	C84_RTN	C132_RTN	C180_RTN	C228_RTN
2	C36_IN	C84_IN	C132_IN	C180_IN	C228_IN
3	Relay 6 NO	Relay 14 NO	Relay 22 NO	Relay 30 NO	Relay 38 NO
4	C35_RTN	C83_RTN	C131_RTN	C179_RTN	C227_RTN
5	C35_IN	C83_IN	C131_IN	C179_IN	C227_IN
6	Relay 6 NO	Relay 14 NO	Relay 22 NO	Relay 30 NO	Relay 38 NO
7	Relay 6 NC	Relay 14 NC	Relay 22 NC	Relay 30 NC	Relay 38 NC
8	Relay 6 NC	Relay 14 NC	Relay 22 NC	Relay 30 NC	Relay 38 NC
G-J1					
1	C38_RTN	C86_RTN	C134_RTN	C182_RTN	C230_RTN
2	C38_IN	C86_IN	C134_IN	C182_IN	C230_IN
3	C39_RTN	C87_RTN	C135_RTN	C183_RTN	C231_RTN
4	C37_IN	C85_IN	C133_IN	C181_IN	C229_IN
5	C37_RTN	C85_RTN	C133_RTN	C181_RTN	C229_RTN
6	C39_IN	C87_IN	C135_IN	C183_IN	C231_IN
7	C40_RTN	C88_RTN	C136_RTN	C184_RTN	C232_RTN
8	C40_IN	C88_IN	C136_IN	C184_IN	C232_IN

Table E-1
Contact Module Connector Pinouts for Each Slot (cont.)

G-J2					
1	C42_RTN	C90_RTN	C138_RTN	C186_RTN	C234_RTN
2	C42_IN	C90_IN	C138_IN	C186_IN	C234_IN
3	Relay 7 NO	Relay 15 NO	Relay 23 NO	Relay 31 NO	Relay 39 NO
4	C41_RTN	C89_RTN	C137_RTN	C185_RTN	C233_RTN
5	C41_IN	C89_IN	C137_IN	C185_IN	C233_IN
6	Relay 7 NO	Relay 15 NO	Relay 23 NO	Relay 31 NO	Relay 39 NO
7	Relay 7 NC	Relay 15 NC	Relay 23 NC	Relay 31 NC	Relay 39 NC
8	Relay 7 NC	Relay 15 NC	Relay 23 NC	Relay 31 NC	Relay 39 NC
H-J1					
1	C44_RTN	C92_RTN	C140_RTN	C188_RTN	C236_RTN
2	C44_IN	C92_IN	C140_IN	C188_IN	C236_IN
3	C45_RTN	C93_RTN	C141_RTN	C189_RTN	C237_RTN
4	C43_IN	C91_IN	C139_IN	C187_IN	C235_IN
5	C43_RTN	C91_RTN	C139_RTN	C187_RTN	C235_RTN
6	C45_IN	C93_IN	C141_IN	C189_IN	C237_IN
7	C46_RTN	C94_RTN	C142_RTN	C190_RTN	C238_RTN
8	C46_IN	C94_IN	C142_IN	C190_IN	C238_IN
H-J2					
1	C48_RTN	C96_RTN	C144_RTN	C192_RTN	C240_RTN
2	C48_IN	C96_IN	C144_IN	C192_IN	C240_IN
3	Relay 8 NO	Relay 16 NO	Relay 24 NO	Relay 32 NO	Relay 40 NO
4	C47_RTN	C95_RTN	C143_RTN	C191_RTN	C239_RTN
5	C47_IN	C95_IN	C143_IN	C191_IN	C239_IN
6	Relay 8 NO	Relay 16 NO	Relay 24 NO	Relay 32 NO	Relay 40 NO
7	Relay 8 NC	Relay 16 NC	Relay 24 NC	Relay 32 NC	Relay 40 NC
8	Relay 8 NC	Relay 16 NC	Relay 24 NC	Relay 32 NC	Relay 40 NC

■ SPECIFICATIONS

External Input Power	No external power is required. Sense voltage is generated on daughter board at +24Volts DC
Temperature Range	0 C° Min to 60 C° Max
Input Contact Sense Levels	Off (0) < +5 VDC On (1) +18 VDC < X < + 40 VDC
Number of Inputs	6 contact inputs and 1 relay output per module 48 max inputs and 8 outputs per daughter board
Type of Input	All inputs must be isolated contacts
Number of Outputs	1 DPDT Relay per connector/ 1 connector/ interface (one N.O. pair and one N.C. pair) 8 relay contacts per daughter board
Type of Output	Isolated relay contacts capable of 1 Amp @ 125 Volts AC or 1 Amp @ 24 Volts DC
I/O Noise Suppression	Each I/O has series inductors and MOVs for noise suppression and ESD protection.

SPANNING TREE PROTOCOL

F

A catenet is a network of LANs connected by bridges to emulate a large LAN. For proper operation, the catenet must have a tree structure, that is, there must be only one path from any host to any other host in the catenet. If there are multiple paths, it is possible for multiple copies of frames (especially multicasts) to reach a host. Worse, it is possible for frames to reproduce without bound.

The Spanning Tree Protocol (STP) eliminates multiple paths in a bridged catenet by blocking ports that create those paths. It imposes a tree structure on the catenet so that there is only one path between each pair of hosts.

The root bridge is the root of the spanning tree. It is the bridge with the numerically smallest bridge identifier, which consists of a user-assigned priority prefixed onto the bridge's unique MAC address. The user can assign small priority numbers to primary bridges and large priority numbers to backup bridges, or can leave them with a default value and let their MAC addresses determine the root bridge.

Each LAN has a designated bridge, which is the bridge connected to the LAN that has the shortest path to the root bridge. The port of the designated bridge that is connected to the LAN is called the designated port. All traffic on the LAN that goes towards the root bridge passes through the designated port of the designated bridge.

Each bridge (except for the root bridge) has a root port, which is the bridge's port that has the shortest path to the root bridge.

The shortest path from a bridge to the root bridge is calculated by assigning a cost to each root port. This "cost" depends on the bandwidth of the LAN connected to that port. Fast ports (1 Gbps, 100 Mbps) have lower cost than slow ports (10 Mbps). The path cost from a bridge B to the root bridge is the sum or the costs of the root ports between B and the root bridge.

To summarize, a spanning tree has one root bridge selected by its bridge identifier. Each non-root bridge has a root port that has the shortest path to the root bridge. Each LAN has a designated bridge and designated port that has the shortest path to the root bridge. All ports of the root bridge are designated ports of the LANs connected to the root bridge. Non-root bridges may have any number of designated ports, including zero. (This occurs if all LANs connected to that bridge have a shorter path to the root bridge through other bridges.)

Each host in the catenet has a single path to the root bridge through designated ports and root ports, and therefore a single path to any other host in the catenet.

Only root ports and designated ports carry data traffic. This imposes a tree structure on data traffic so there cannot be loops. All other bridge ports are alternate ports: they block data traffic but are available as backup ports if primary ports fail.

The spanning tree is constructed using a robust distributed algorithm called the Spanning Tree Protocol. Frames called Bridge Protocol Data Units (BPDUs, pronounced “bippy-doos”) carry STP data between bridges on a LAN. BPDUs are multicasts with group address 01.80.C2.00.00.00. BPDUs are received and transmitted by all bridge ports, including alternate ports. They are originated and terminated by bridges on a single LAN; they are never forwarded. BPDUs are ignored by non-bridge hosts.

There are two kinds of BPDUs. A configuration BPDU (config BPCU) is transmitted by the root bridge every hello time (default 2 seconds) on all its ports. The config BPDU identifies the root bridge and the path cost to the root bridge, along with other parameters.

A non-root bridge receives a config BPDU on its root port. It adds its root port cost to the path cost and then transmits the modified config BPDU on its designated ports. The modified config BPDU identifies the designated bridge and designated port.

Within a few hops, all bridges in the catenet receive (modified) copies of the config BPDU. The LAN bandwidth is negligible: one config BPDU per hello time per LAN.

When it receives a config BPDU, each bridge examines it to see if it should change the spanning tree's topology. In the steady state, there is no need to change it. However, when a link is added to or deleted from the catenet, the current spanning tree may no longer be optimal.

First, the bridge looks to see if it has a better claim to be the root bridge, i.e., its bridge identifier is numerically less than the config BPDU's bridge identifier. It also checks whether it has an alternate port that should become the designated port of its incident LAN because this bridge has a lower cost path to the root. In addition, a bridge may stop receiving config BPDUs on its root port due to a recently failed connection.

In any of these cases, the bridge initiates topology change (TC). In a topology change, designated and root ports become alternate ports and vice versa. However, we have to do this carefully so that we do not have temporary loops in the catenet. Instead of switching immediately, ports go through several states:

Forwarding	A forwarding port is a root or designated port. It can forward data traffic. A topology change can convert it immediately to blocking.
Listening	A listening port does not pass data traffic. It receives and transmits BPDUs to confirm that it should indeed become a designated or root port. If it receives BDPUs that suggest otherwise, it goes back to blocking. If it still thinks it should become a designated or root port after a forward delay (default 15 seconds), it sets itself to learning.
Learning	The learning state is the same as listening, except that the port receives data frames and uses them to update the bridge's MAC address table so that the bridge knows which port is associated with a MAC address. This reduces flooding due to

unknown MAC addresses when the port comes up. The data frames are discarded. After the forward delay, the port enters the forwarding state.

(There is also a disabled state where the port is manually disabled by bridge management.)

Normally, bridges age out MAC addresses very slowly, e.g., they forget a MAC address if it hasn't been seen as a source address in 5 minutes. When a topology change occurs, MAC addresses may move from one bridge port to another. To prevent stale port assignments, the MAC address table is aged very quickly when topology change is in effect. Specifically, it is aged within the forward delay (default 15 seconds).

When a bridge initiates a topology change, it sends a topology change BPDU (TC BPDU) to the current root bridge. The root bridge then sets a TC flag in all config BPDUs for a period of time. This ensures that all bridges know there is a topology change in action and age their filtering databases quickly.

GLOSSARY

A

Abbreviated Address: A brief code used to represent a conventional address. The device translates the abbreviated address into the full address and appends appropriate codes. Syn.: Mnemonic address

ACSE: Association-Control Service Element

Address: The symbol, code, or text sequence that identifies the origin and/or the destination of a data communications message and/or segments of messages.

Adjacency: An adjacency is formed between the DR and all nondesignated routers on a broadcast or NBMA network. An adjacency is also formed between the BDR and all non designated routers. OSPF routing updates are sent and received only on adjacencies.

Alphanumeric: A set of characters comprised of both letters and numbers.

Alternate Routing: A feature of switching devices in which a given call is routed over alternate paths or circuits when an initially chosen path, circuit, or service is unavailable.

Area: A set of contiguous networks and hosts within the AS. An area also includes all routers that interface with any of the included networks. The topology of an area is hidden from the rest of the AS, which permits a significant reduction in routing traffic. Each area maintains its own topological database.

Area border router (ABR): A router that has an interface in more than one OSPF area.

Asynchronous Transfer Mode (ATM): A high-speed connection-oriented multiplexing and switching protocol that uses fixed-length cells to support multiple types of traffic.

Asynchronous Transmission: A method of data transmission that allows characters to be sent at irregular intervals by preceding each character with a start bit and following it with a stop bit. Such a method does not require the clocking of signals. Ant.: Synchronous Transmission

Authentication Header (AH): An IPSec protocol that defines methods of establishing the identity of the message originator and ensures that the transmitted data has not been tampered with.

Autobaud: A feature of some devices in which means are provided to detect the data rate in use in an incoming call and adjust to it without previous knowledge or operator intervention. Syn.: Automatic Data Rate Detection

Autocall: The process of automatically dialing a telephone number, as by a computer, to begin a data communications session.

Automatic Route Selection: The ability of a device to select the optimum route for a call without operator intervention.

Autonomous System (AS): A group of routers that exchange routing information via a common routing protocol.

Autonomous system border router (ASBR): An OSPF router that connects to another AS that is running a different IGP than OSPF.

B

Backbone network: The backbone of an AS consists of all networks that are contained in any area, along with their attached routers and all area border routers. The backbone components must be contiguous (in some cases, they are joined by virtual links). The backbone is responsible for distributing routing information between areas (inter-area routing). Its properties are similar to those of an area, in that the backbone topology is invisible to each of the areas, and, conversely, the backbone knows nothing of the area topologies.

Backup designated router (BDR): Router that will take over the role of DR in the event the DR fails.

Backward Explicit Congestion Notification (BECN) Bit: When set in a frame relay frame, this bit notifies the source that congestion is occurring.

Basic Rate Interface (BRI): An ISDN service that provides two B-channels for user data, each at 64 kbps, and one D-channel at 16 kbps for signalling information.

Battery Backup: A battery that provides power to the system to avoid the loss of data when the main power fails.

Baud: A unit of transmission speed. The number of discrete signal elements transmitted in one second. Below 300 baud, baud = bits per second; above 300 baud, more than one bit can be placed on a baud through coding techniques.

B-Channel: The ISDN “bearer” channel that carries user data.

Binary Coded Decimal: A four-bit encoding scheme for digits 0 through 9.

Bit: A binary digit, the representation of a signal as either a binary zero or a one.

Bit-Oriented: A link control protocol characterized by the encoding of control information into specific bit fields and by the general transparency of the data field.

Bit Rate: The transmission speed of a communications facility or device, normally expressed as bits per second (bps).

Bits Per Second (bps): The number of bits transmitted or received each second.

Block: A unit of data consisting of multiple bits or multiple characters sufficiently delimited and self-contained to permit such functions as error control, routing, buffering, and retransmission to be performed on it as a discrete entity.

Block Check Character: A character or set of characters appended to a transmitted block of data to assist in error detection.

Break: 1) An interruption in transmission. 2) A signal used to cause this to happen.

Bridging: The ability to store and forward packets on LANs without the use of the network layer.

Broadcast: A transmission technique in which a message is sent to the entire population of potential receivers or to a major group of receivers.

Broadcast network: A network that supports more than two attached (multiaccess) routers, and that can address a single broadcast message to all attached routers. Example: an Ethernet network or Token-Ring LAN.

Buffer: A temporary storage location for data being sent or received, usually located between two different devices that have different abilities or speeds for handling the data.

Bus: A transmission path, usually short and very high-speed in operation.

Byte: A quantity of information (generally 8 bits), used mainly in referring to data storage. Syn.: Character, Octet

C

Call Barring: The ability to prevent all or certain calls from being accepted.

Carrier: An electrical signal at a continuous frequency capable of being modified to carry information.

Carrier Detect (CD): A signal indicating that the device has detected the carrier signal.

Central Processing Unit (CPU): The section of a system responsible for receiving and executing coded instructions. Syn.: Communications Processor Unit.

Challenge Handshake Authentication Protocol (CHAP): An authentication mechanism that can be negotiated on a PPP link to identify the remote end. CHAP is based on a shared “secret” that is configured in both units but never transmitted.

Channel: A path over which information flows.

Character: Standard bit representation of a symbol, letter, or number. Syn.: Byte.

Character-Oriented: A link control protocol in which block delimiting and supervisory actions are based on the presence or absence of certain control characters in the communication stream and in which block content usually consists of character data.

Check Bit: A bit added to a unit of data to perform an accuracy check.

Checksum: A form of block check character, the content of which is derived from the content of a transmission block through an additive process.

Clear-to-Send (CTS): A modem control signal indicating that the connected terminal is ready to transmit data.

Clock: 1) An oscillator-generated signal that provides a timing reference for a transmission link; used to control the timing of functions such as sampling interval, signaling rate, and duration of signal elements. 2) In data processing, a quartz-generated pulse or strobe that sets the rate of logic functions.

Closed User Group (CUG): A subgroup of users in a network configured such that communication to and/or from the group is restricted.

Cold Start: The restarting of equipment after dumping of battery backed memory (which results in the resetting of parameter values to factory defaults).

Committed Information Rate (CIR): The transfer rate that the frame relay network is committed to transfer under normal operating conditions.

Compression: A technique that reduces the number of data bits being transmitted, thereby saving bandwidth.

Connection: A path between devices that allows the transmission of data.

Connectionless Network Protocol (CLNP)

Connectionless Network Service (CLNS): Indicates an X.25 connectionless OSI transport bridge. Used for TL1 7/3 conversions.

Connection-oriented Network Service (CONS): An X.25 connection-oriented OSI transport bridge.

Connector: A physical interface, such as RJ-69 or EIA RS-232C, typically with male and female components.

Control Characters: 1) Any extra transmitted characters used to control or facilitate data transmission between data terminals. 2) Characters transmitted over a circuit that are not message or user data, but that cause certain control functions to be performed when encountered; includes extra characters associated with addressing, polling, message delimiting and blocking, framing, synchronization, and error checking.

Cyclic Redundancy Check Character: A form of block checking in which a block of information is divided by a special binary polynomial with the remainder transmitted along with the original block; the combination when divided again by the same polynomial at the receiving station indicates whether an error has occurred in transmission.

D

Data Circuit Terminating Equipment (DCE): The equipment that produces the clock signal in a synchronous communication link. The DCE is normally the network side of the connection.

Data Link: Any serial data communications transmission path, generally between two adjacent nodes or devices, and without any intermediate switching nodes.

Data Link Connection Identifier (DLCI): A level 2 address used to route frame relay traffic.

Data Link Layer: The network processing entity that establishes, maintains, and releases data link connections between (adjacent) elements in a network.

Data Network Identification Code (DNIC): A 4-digit number that uniquely identifies a public packet data network.

Data Terminal Equipment (DTE): The equipment that receives the clock signal in a synchronous communication link. The DTE is normally the terminal.

Data Transfer Rate: The average number of bits, characters, or blocks per unit of time transferred from a data source to a data sink.

Dataphone Digital Service (DDS): A Bell System standard developed for delivering synchronous data over a dedicated 4-wire circuit.

D-Channel: The ISDN “delta” channel, which is used to carry signaling information.

Dedicated Line: A private or leased line. Syn.: Dedicated Circuit

Default: The preset factory value.

Designated router (DR): On broadcast and NBMA networks, the designated router is used to flood link-state information to the common network.

Destination Service Access Point (DSAP): A designation to help define the recipient of a packet.

Diagnostic Port: An ACT Networks software feature for configuration of products, retrieval of diagnostics, and compilation of statistics.

Dial-Up: The use of a dial or push-button instrument to initiate a call on the public switched network, or a similar operation carried out by a machine.

Digital: 1) Communications procedures, techniques, and equipment where information is encoded as either a binary “1” or “0”. 2) The representation of information in discrete binary form, discontinuous in time.

Digital Loopback: A technique for testing the digital processing circuitry of a communications device. The device being tested echoes a received test message after first decoding and then re-encoding it. The echoed message is compared with the original message.

Digital Signaling: Transmission of digital data.

Digital Switching: Establishing and maintaining a connection, under stored program control, where binary-encoded information is routed between an input and an output port.

Discard Eligibility (DE) Bit: A bit in the frame relay header that, when set, indicates that the frame is a preferential candidate for discard under congested conditions.

Disconnect: The breaking or release of a circuit connection.

Download: Receiving data from another computer. Ant.: Upload

E

Echo: A reflection of an outgoing signal to the transmitter.

Emulation: The ability of one device to imitate the operation, interface, or other behavior of another device.

Encapsulated Security Payload (ESP): An IPSec protocol that defines methods of establishing the identity of the message originator, ensures that the transmitted data has not been tampered with, and defines encryption methods for the data.

Encapsulation: Placing a protocol's packet completely inside another protocol's packet.

Erasable Programmable Read-Only Memory (EPROM): Component for program storage; can be erased and reprogrammed under controlled conditions.

Error Control: The mechanism provided in a communication for the detection and correction of errors that occur during transmission.

Escape Code: In character-oriented protocols, a specific code that designates the characters following it as having a significance that is different from that which they normally have.

Ethernet: The original CSMA/CD LAN invented by Xerox and standardized by Digital, Intel, and Xerox. Now referenced as IEEE 802.3.

Extended Addressing: In many bit-oriented protocols, a facility allowing for the use of larger addresses than normal; may be required in extensive networks.

External routes: Routes learned from another AS or from another routing protocol can be injected into OSPF as external routes. There are two types of external routes. A type 1 external route has a cost that includes the OSPF cost plus the cost from the ASBR to the network. A type 2 external route

has a cost equal only to the cost from the ASBR to the external network.

F

Facility: An operational capability or the means of providing a capability.

Fast Select: 1) A facility that applies to virtual calls that allows the DTE to increase the possibility of transmitting data in call setup and call clearing packets beyond the basic capabilities of a virtual call. 2) In packet switched networks, a calling method that allows the user to send a limited amount of information along with a call request packet rather than after the packet.

Flag: A bit pattern of 6 consecutive “1” bits used to designate the beginning or end of a transmission in protocols such as High-Level Data Link Control (HDLC).

Flooding: Used to distribute and synchronize link-state databases between routers.

Hello Protocol: OSPF nodes communicate with adjacent nodes using Hello Protocol. Hello protocol involves sending test messages to adjacent nodes and tracking their state. Once an initialization phase is passed and adjacency is established, two routers can exchange routing information.

Flow Control: The prevention of data overload within a communications network or in an information processor, accomplished by limiting data flow according to some algorithm.

Forward Explicit Congestion Notification (FECN) Bit: When set in a frame relay frame, notifies the destination that congestion is occurring.

Frame: A group of bits sent serially; a logical transmission unit.

Frame Check Sequence (FCS): In bit-oriented protocols, a 16-bit field added to the end of a frame and that contains transmission error-checking information.

Frame Relay: A data communications protocol that dispenses with much of the overhead for error control embodied in X.25.

G

Ground: Any electrical connection or common conductor that, at some point, connects to the earth or other object of neutral potential.

H

Header: The portion of a transmission frame or block that contains control information.

Hexadecimal: Base 16 numbering.

High-Level Data Link Control (HDLC): The standard protocol for data communications specified by CCITT. A bit-oriented protocol in which control information is always placed in the same position, and in which the control information bits differ from those used to represent data.

Hunt Group: A series of communications lines organized in such a way that if the first is busy, the search continues until a free one is found.

I

Input/Output (I/O): Information received (input) or transmitted (output) by a particular device.

Integrated Services Digital Network (ISDN): A digital communications system designed to transmit both voice and data, as well as any other kind of digital communication.

Intelligent Electrical Device (IED): A blank term that covers many types of equipment in a substation environment.

Interarea routing: Routes between two different OSPF non-backbone areas. The interarea path consists of three parts: the intra-area path from the area to the ABR of the source area, the backbone path from the source ABR to the destination

ABR, and finally, the path from the destination ABR to the destination network.

Interface: Connection between a router and a network with a single IP address and subnet mask. Also referred to as a link. (2) A mechanical or electrical link connecting two or more pieces of equipment.

Internet: A network connecting many computers and computer communities throughout the world.

Internet Key Exchange (IKE): A type of security association that provides negotiation, peer authentication, key management, and key exchange.

Internet Protocol (IP): A packet protocol for communicating over LANs.

Intra-area routing: Routes between networks in the same area. These routes are based only on information received from within the area.

IP Security (IPSec): A comprehensive set of Layer 3 VPN components for IP networks.

IPsec Security Association (IPSec SA): A unidirectional type of security association.

IPX: A protocol that allows asynchronous devices to connect to a Novell Netware LAN.

ITU-T: The international consultative committee that develops standards for the telecommunications industry. Formerly called the Consultative Committee of International Telegraph and Telephone (CCITT).

J

Jumper: A wire used to connect two terminals, for example, on a circuit board.

L

Layer: A collection of related network processing functions that comprise one level of a hierarchy of functions. Functions in the same layer coordinate their actions via protocols, while

functions in adjacent layers coordinate their actions via interfaces.

Light Emitting Diode (LED): A device that accepts electrical signals and converts the energy to light.

Link: A communications channel or circuit.

Link Access Procedure (LAP): The original data link level protocol specified in the CCITT X.25 interface standard. It has since been supplemented by LAPB.

Link Access Procedure Balanced (LAPB): The data link level of X.25.

Link Layer: 1) The logical entity in the OSI model concerned with transmission of data between adjacent network nodes. 2) The second layer in the OSI model, between the physical (first or foundation layer) and the network layers.

LLC (Link Level Control): A protocol that provides sequencing, error checking, and flow control services to SNA within a LAN environment.

Link-state advertisements (LSA): Describes the local state of a router.

Local Management Interface (LMI): A specification that provides enhanced support for frame relay PVCs. The features were later incorporated into the CCITT and ANSI standards.

Logical Channel: In packet mode of operation, a means of two-way simultaneous transmission across a data link that is comprised of associated transmit and receive channels.

Logical Channel Number: A means of identifying a virtual circuit.

Logical Connection: A virtual circuit established by machine logic.

Loopback: A diagnostic procedure used for transmission devices; a test message is sent to a device being tested, and is then sent back to the originator and compared with the original transmission.

M

M-bit: An X.25 feature, or facility, that notifies the receiver that not all data from the sender (or the transport layer) has been transmitted. Syn.: More Bit

Media Access Control (MAC): The lower half of Layer 2 of the OSI reference model.

Management Information Base (MIB): A database of network management information used with SNMP.

Mnemonic Address: A brief code used to represent a conventional address. The device translates the abbreviated address into the full address and appends appropriate codes. Syn.: Mnemonic address

Modulus: 1) The quantity of messages or frames that can be counted before the number resets to zero. 2) The number of messages (N-1) that can be outstanding from a transmitter before an acknowledgment is required from the receiver.

Multilink: A capability of an ISDN line in which the two B-channels can be bundled together to provide additional bandwidth if required.

Multipoint: A line or circuit that interconnects several stations with a central point.

N

NCP (Network Control Program): The software for the Front End Processor in an SNA environment.

Neighboring routers: Routers with an interface to a common network.

Network: Three or more points connected, or connectable, by communication paths, organization of functions, and the description of data formats and procedures.

Network Element (NE): Any discrete item in the network.

NET (Network Entity Title)

NSAP (Network Service Access Point)

Network User Identification (NUI): An identification, similar to a password, that may be required over X.25 lines, particularly dial-up lines.

Node: A discrete termination point in a network at which data can flow onto and/or off the network from/to user devices and systems.

Nonbroadcast network: Supports more than two attached routers but has no broadcast capability. Frame relay and X.25 are examples of nonbroadcast networks. There are two general types of nonbroadcast networks, nonbroadcast multi-access (NBMA) and point-to-multipoint. The differences between the two depend more on the configuration of routers than on the physical network.

Nonvolatile Storage: Any storage medium or circuitry that does not lose its contents when power is turned off or lost.

NRZ/NRZI (Non-Return to Zero/Non-Return to Zero Inverted): Coding used to represent the signaling on a line.

Null: A control character without meaning that is used to pad transmissions to comply with format and timing requirements.

O

OSI (Open Systems Interconnection): A seven-layer logical structure for network operations.

OSPF (Open Shortest Path First): A routing scheme that operates over IP protocol. OSPF is a link state metric protocol that makes routing decisions based on link capacity, delay and throughput requirements, the number of data units presently in queue for transmission over a particular link, the number of hops required to reach a destination, and the ability to reach gateways and routers along the route. To take network dynamics into account, OSPF includes a weighting factor for each route. OSPF is considered a more robust protocol than RIP, which makes routing decisions based only on the number of hops to a destination.

P

Packet: A single unit of information, including data and control elements, that is passed between adjacent nodes.

Packet Assembler-Disassembler (PAD): 1) A network interface device that allows multiple asynchronous and/or synchronous terminals or host computer ports to interface to a packet-switching network. 2) A protocol conversion device that allows user terminals not equipped for packet switching to communicate over an X.25-based channel.

Packet Switching: A data transmission technique in which user information is segmented and routed in discrete data envelopes called packets, each with its own appended control information for routing, sequencing, and error checking.

Packet Switching Network: A network designed to operate by means of packet switching.

Parallel: A transmission mode in which all the data bits in a character are sent at once over eight parallel paths.

Parity: In ASCII, a check of the total number of “1” bits in a character. A final eighth bit is set so the count when transmitted is always even or always odd.

Parity Bit: A binary bit appended to an array of bits to make the sum of all the bits always odd or always even.

Parity Check: A process of error checking using the parity bit.

Password Authentication Protocol (PAP): An authentication mechanism that can be negotiated on a PPP link. PAP is based on a shared password that is transmitted over the line.

Permanent Virtual Circuit (PVC): A connection between two endpoints that is permanently maintained.

Physical Layer: Within the OSI model, the lowest level of network processing, concerned with the electrical, mechanical, and handshaking procedures that connect a device to a transmission medium.

Proxy LAN Physical Unit (PLPU): The representation of the control unit (CU) over the network.

Point-to-Point: A description of a circuit that connects two points directly with (usually) no intermediate processing nodes or computers, although there may be switching facilities.

Point-to-Point Network: A network that joins a single pair of routers. A point-to-point network is considered a single network, no matter how many IP network/subnet numbers are assigned to it. Example: a serial line running at 64 kbps.

Point-to-Point Protocol (PPP): A data link layer protocol that provides a point-to-point link with multiplexing capability for use in the IP community.

Polling: The process by which the master/primary station sequentially gives each of a set of slave/secondary stations the opportunity to transmit by successively addressing each with a poll inquiry.

Polling Delay: The elapsed time between successive polls to a given station.

Port: 1) A point of access into a computer, a network, or other electronic device. 2) The physical or electrical interface through which one gains access.

Port Sharing: 1) An arrangement by which a port in one device is used consecutively by two or more devices. 2) For routing, an arrangement whereby a particular routing configuration is used by more than one port.

Primary Rate Interface (PRI): An ISDN service that provides connections at T-1 or E-1 speeds.

Private Network: A network established and operated by a private organization or corporation for its exclusive use. Ant.: Public Network

Profile: A set of X.3 parameters and their values.

Programmable Read-Only Memory (PROM): Components that contain system startup and operating default programs.

Programming Plug: A component that changes the physical presentation of signals to accommodate a physical DTE or a physical DCE connection.

Protocol: A set of standard rules governing the cooperation and interaction between corresponding peer entities.

Public Data Network (PDN): A network designed primarily for data transmission and intended for many users from many organizations.

Public Switched Telephone Network (PSTN): A dial-up phone network.

R

Random Access Memory (RAM): Read/Write memory (generally temporary) used for the storage of programmable code, buffers, and so on.

Read-Only Memory (ROM): 1) A data storage device whose contents cannot be altered, except under certain circumstances. 2) Permanent storage.

ROSE (Remote Operations Service Element)

Route summarization: Routes within an area, routes from another AS, and routes learned from another routing protocol can be summarized by OSPF into a single route advertisement if the IP network was designed properly. Summarization can occur only on an ABR or an ASBR. Summarization is not automatic.

Router ID: A 32-bit number used to identify each router. Typically the highest IP address assigned to the router. If loopback interfaces are used on the router, then the router ID is the highest IP address of the loopback interfaces regardless of the value of the IP address for the physical interfaces.

Routing: The function of selecting the appropriate path(s) for the movement of data within a network, ensuring that all inputs are directed to their appropriate destination(s).

Routing Information Protocol (RIP): A routing protocol commonly used for routing IP packets, RIP determines routes based on distance, with no consideration of the state of the links or nodes that must be used to reach a destination. (Compare OSPF.)

S

Security Associations: A method for establishing trust between two devices in a peer-to-peer relationship that enables VPN endpoints to agree on a set of conversational rules by negotiating policies with a potential peer.

Serial: The movement of information one bit at a time.

Serial Line Interface Protocol (SLIP): A protocol that allows remote terminals to establish an asynchronous connection to a network.

Service Access Point (SAP): The address of the user of a service.

Session: A bounded series of events between two parties in which communication takes place.

Simple Network Management Protocol (SNMP): A standardized network management system that is based on providing certain information to the MIB.

SNPA (Sub-Network Point of Attachment)

Software: Generic term for computer programs.

Source Service Access Point (SSAP): A means for identifying the origination of a packet.

Space: The binary 0 condition.

Start Bit: In asynchronous transmission, the first element in each character that prepares the receiving device to recognize the incoming information.

Start-Stop Transmission: Asynchronous transmission of a group of data elements that is preceded by a start and followed by a stop signal.

Station: A device that is capable of being the origin or destination of data.

Stop Bit: In asynchronous transmission, the last transmitted element in each character, which permits the receiver to come to an idle condition before accepting another condition.

Stub Network: A network that has a local endpoint and is not bidirectionally connected in the OSPF database topology.

Subnetting: Division of the network into smaller areas. When used with IP addresses, the subnet for class A addresses is the bottom three octets of the address; for class B addresses, the bottom two octets; and for class C, the bottom one octet.

Switched Virtual Circuit (SVC): A connection between two endpoints that is set up on an as-needed basis and taken down when the call is completed.

Synchronization Bits: Framing bits in synchronous transmission.

Synchronous Data Link Control (SDLC): IBM's version of a bit-oriented data link control protocol.

Synchronous Transmission: Transmission in which the data characters and bits are transmitted at a fixed rate with the transmitter and receiver synchronized, eliminating the need for start-stop elements.

Syntax: The rules of form governing code groups.

System Network Architecture (SNA): The layered structure and protocol for data transmission in an IBM network.

T

TARP (TID Address Resolution Protocol)

TCP-IP (Transmission Control Protocol/Internet Protocol): A term often used to describe the Internet suite of protocols, although technically speaking there are other protocols within the suite.

Telnet: A terminal emulation application that allows users to log in to a remote host.

Terminal: A point in a network through which data can either enter or leave. Syn.: Data Terminal Equipment (DTE)

Time-out: Specific delays designed into various control functions intended to ensure that, absent some response from a remote station, the local station will not hang up in some unknown logical state.

TL1 (Transaction Language 1): A language commonly used for Operations and Support.

Token Ring: A LAN standardized within 802.5 and FDDI.

Topology: The physical geometry of a network.

TP0, 1, 2, 3, or 4: Transport protocol class 0, 1, 2, 3, or 4.

Transit Area: The area through which virtual link traffic passes.

Transit Network: A network that routes traffic that is neither locally originated nor locally destined.

Translation: The conversion of an address into another address that will be compatible on another network.

Transparency: A condition in which a communication or computer system is designed to be oblivious to and independent of the content of data.

Transport Mode: A method of sending IPSec data in which only the IP payload is cncrypted.

Trunk: A transmission path of one or more channels between switching and concentration/distribution equipment.

Tunnel Mode: A method of sending IPSec data in which the entire datagram is encrypted.

V

V.24: CCITT definitions for moderate speed physical interchange circuits between DTE and DCE; similar to EIA RS-232.

V.32: CCITT standard for dial-up data communications transfer.

V.35: CCITT standard for high speed (> 19.2 kbps) physical interchange circuits between DTE and DCE.

Virtual Call: A call that makes use of a virtual call capability.

Virtual Call Capability: 1) A user facility in which a call setup procedure and a call clearing procedure determine a period of communication between two DTEs in which the

user's data are transferred in the network in a packet mode of operation. All of the user's data are delivered from the network in the same order in which they were received by the network. 2) Setup and clearing on a per call basis where each call appears to have a dedicated connection for the duration of the call.

Virtual Circuit: 1) A communications arrangement in which data from a source user is transferred to a destination user over various real circuit configurations during a single period of communication. 2) In a packet switched network, an end-to-end transmission path with different user packets sharing the path. Syn.: logical circuit; phantom circuit. Ant.: physical circuit

Virtual Channel Identifier (VCI): In conjunction with the VPI, a means of identifying a virtual circuit in a frame relay network.

Virtual Link: Links that belong to the backbone network and are used to restore backbone connectivity. Their discontiguous endpoints are joined by a defined transit area.

Virtual Path Identifier (VPI): In conjunction with the VCI, a means of identifying a virtual circuit in a frame relay network.

Virtual Private Network (VPN): A method for providing secure exchanges with remote offices, vendors, and partners through the use of encrypted transmissions using key exchanges, hasing, and encryption algorithms.

VTAM (Virtual Terminal Access Method): An SNA protocol.

W

Warm Start: The restarting of equipment without dumping the battery backed memory. Operating parameters are left intact, but packets in the process of being received, queued, or transmitted are lost.

Window: A flow control mechanism whose size is equal to the number of frames, packets, or messages that can be sent

from a transmitter to a receiver before a reverse acknowledgment is required.

X

X.121: The ITU-T recommended method for employing a 15-digit addressing standard for worldwide communications with the X.25 packet protocol.

X.21: 1) A line communications standard established by the ITU-T for synchronous transmission. 2) The physical interface description of X.25. 3) In Europe, the method of connecting higher speed X.25 trunks.

X.21bis: A modification of the X.21 standard; identical to RS-232C at the physical level. This is the method employed to connect lower speed (< 19.2 kbps) devices worldwide.

X.25: A three-layer protocol defined by the ITU-T built using the existing standards for X.21 and HDLC to specify the two lower level protocols. X.25 is a packet switched protocol in use for data communications worldwide.

X.28: DTE/DCE interface for start-stop mode data terminal equipment accessing a packet assembly/disassembly facility (PAD) in a public data network located in the same country.

X.29: Procedures for the exchange of control information and user data between a packet assembly/disassembly facility (PAD) and packet node DTE or anotherPAD.

X.3: Packet assembly/disassembly (PAD) facility in a public data network. Defined by the ITU-T and used in X.25.

X.75: The ITU-T recommendation for the interconnection and interoperation of two packet switched public data networks, both of which support the X.25 user interface.

X-On/X-Off: A commonly used flow-control protocol.

XID (Exchange Identification): A type of unnumbered information command used to set up exchange parameters between LLC entities.

XOT: A method for transporting X.25 over a TCP-IP network.

Numerics

A

INDEX

INDEX

B

C

INDEX

D

F

INDEX

G

H

I

INDEX

INDEX

N

O

P

INDEX

Q

R

S

T

INDEX